



<p>(51) 国際特許分類 H04N 1/387</p>	<p>A1</p>	<p>(11) 国際公開番号 WO97/49235</p> <p>(43) 国際公開日 1997年12月24日(24.12.97)</p>
<p>(21) 国際出願番号 PCT/JP97/00395</p> <p>(22) 国際出願日 1997年2月13日(13.02.97)</p> <p>(30) 優先権データ 特願平8/159330 1996年6月20日(20.06.96) JP</p> <p>(71) 出願人 (日本についてののみ) 日本アイ・ビー・エム株式会社(IBM JAPAN LTD.)(JP/JP) 〒106 東京都港区六本木3丁目2番12号 Tokyo, (JP)</p> <p>(71) 出願人 (日本を除くすべての指定国について) インターナショナル・ビジネス・マシーンズ・コーポレーション(INTERNATIONAL BUSINESS MACHINES CORPORATION)(US/US) 10504、ニューヨーク州 アーモンク(番地なし) New York, (US)</p> <p>(72) 発明者 沼尾雅之(NUMAO, Masayuki) 清水周一(SHIMIZU, Shuichi) 森本典繁(MORIMOTO, Norishige) 小林メイ(KOBAYASHI, Mei) 〒242 神奈川県大和市下鶴間1623番地14 日本アイ・ビー・エム株式会社 東京基礎研究所内 Kanagawa, (JP)</p>		<p>(74) 代理人 弁理士 合田 潔, 外(GODA, Kiyoshi et al.) 〒242 神奈川県大和市下鶴間1623番地14 日本アイ・ビー・エム株式会社 大和事業所内 Kanagawa, (JP)</p> <p>(81) 指定国 BR, CA, CN, CZ, HU, JP, KR, PL, RU, SG, SK, 欧州特許 (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).</p> <p>添付公開書類 国際調査報告書</p>
<p>(54)Title: DATA HIDING METHOD AND DATA EXTRACTING METHOD</p> <p>(54)発明の名称 データ・ハイディング方法及びデータ抽出方法</p> <div data-bbox="446 1207 1258 1669"> <p>a ... message array a</p> <p>b ... hiding</p> <p>c ... position P_0</p> <p>d ... position P_1</p> <p>e ... position P_{10}</p> <p>f ... position P_2</p> <p>g ... position P_3</p> <p>h ... position P_4</p> <p>i ... media array M</p> </div> <p>(57) Abstract</p> <p>A data hiding method for hiding message data in media data and a data extracting method for extracting message data hidden in the media data. In the data hiding method, the message data are dispersedly hidden in the media data so that no third person can alter the message data. Specifically, the array elements of a message array are dispersedly hidden in a media array based on a status value S designating a specific array element in the media array when the media data and message data are expressed as the media array and the message array, respectively. The hiding method includes (a) a step of determining the j-th ($j \geq 0$) status value S_j, (b) a step of determining the $(j+1)$-th status value S_{j+1} based on the value S_j, the array element of the media array designated by the value S_j and the above-mentioned array element of the message array, and (c) a step of hiding data to be hidden in the array element of the media array designated by the value S_{j+1}.</p>		

(57) 要約

本発明は、メディア・データ中にメッセージ・データを隠し込むデータ・ハイディング方法及び隠し込まれたデータを抽出するデータ抽出方法に係り、特に、画像や音声といったメディア・データにメッセージ・データを分散して隠し込むことで、第三者がメッセージ・データを改変することが困難なデータ・ハイディング方法を提供することである。具体的には、メディア・データがメディア配列として表現されると共に、メッセージ・データがメッセージ配列として表現されている場合に、メディア配列中の特定の配列要素を指定する状態値 S に基づいて、メッセージ配列の配列要素を分散してメディア配列に隠すデータ・ハイディング方法において、以下のステップを有する点に特徴がある。

(a) j ($j \geq 0$) 番目の状態値 S_j を決定するステップ

(b) j 番目の状態値と、 j 番目の状態値により指定されるメディア配列の配列要素と、前記メッセージ配列の配列要素とに基づいて、 $(j+1)$ 番目の状態値 S_{j+1} を決定するステップ

(c) $(j+1)$ 番目の状態値 S_{j+1} が指定する前記メディア配列の配列要素に対して、ハイディング・データを隠すステップ

参考情報

PCTに基づいて公開される国際出願のパンフレット第一頁に記載されたPCT加盟国を特定するために使用されるコード

AL	アルバニア	ES	スペイン	LR	リベリア	SG	シンガポール
AM	アルメニア	FI	フィンランド	LS	レソト	SI	スロヴェニア
AT	オーストリア	FR	フランス	LT	リトアニア	SK	スロヴァキア共和国
AU	オーストラリア	GA	ガボン	LU	ルクセンブルグ	SL	シエラレオネ
AZ	アゼルバイジャン	GB	英国	LV	ラトヴィア	SN	セネガル
BA	ボスニア・エルツェゴビナ	GE	グルジア	MC	モナコ	SZ	スワジランド
BB	バルバドス	GH	ガーナ	MD	モルドヴァ共和国	TD	チャード
BE	ベルギー	GM	ガンビア	MG	マダガスカル	TG	トーゴ
BF	ブルキナ・ファソ	GN	ギニア	MK	マケドニア旧ユーゴス	TJ	タジキスタン
BG	ブルガリア	GR	ギリシャ		ラヴィア共和国	TM	トルクメニスタン
BJ	ベナン	HU	ハンガリー	ML	マリ	TR	トルコ
BR	ブラジル	ID	インドネシア	MN	モンゴル	TT	トリニダード・トバゴ
BY	ベラルーシ	IE	アイルランド	MR	モーリタニア	UA	ウクライナ
CA	カナダ	IL	イスラエル	MW	マラウイ	UG	ウガンダ
CF	中央アフリカ共和国	IS	アイスランド	MX	メキシコ	US	米国
CG	コンゴ	IT	イタリア	NE	ニジェール	UZ	ウズベキスタン
CH	スイス	JP	日本	NL	オランダ	VN	ヴェトナム
CJ	コート・ジボアール	KE	ケニア	NO	ノルウェー	YU	ユーゴスラビア
CM	カメルーン	KG	キルギスタン	NZ	ニュージーランド	ZW	ジンバブエ
CN	中国	KP	朝鮮民主主義人民共和国	PL	ポーランド		
CU	キューバ	KR	大韓民国	PT	ポルトガル		
CZ	チェコ共和国	KZ	カザフスタン	RO	ルーマニア		
DE	ドイツ	LC	セントルシア	RU	ロシア連邦		
DK	デンマーク	LI	リヒテンシュタイン	SD	スーダン		
EE	エストニア	LK	スリランカ	SE	スウェーデン		

明 細 書

データ・ハイディング方法及びデータ抽出方法

5 [技術分野]

本発明は、メディア・データ中にメッセージ・データを隠し込むデータ・ハイディング方法及び隠し込まれたデータを抽出するデータ抽出方法に関する。

10 [背景技術]

マルチメディア社会の発達により、多くのデジタル化された画像情報や音声情報がインターネット上において、またはCD-ROM、DVD-ROM（またはDVD-RAM）、DVC等の記録媒体として流通されている。これらのデジタル情報は、誰もが簡単に劣化のない完全なコピーを作成することができるため、その不正な使用が問題になってきている。こうした画像データや音声データといったメディア・データを第三者が不法にコピーすることを防止するために、もとのメディア・データに作者の署名といった別の情報をメッセージ・データとして隠し込む（ハイディング）技術が注目されて始めている。デジタル化された画像データ等が違法にコピーされた場合、このコピー中に隠ぺいされた署名を確認しその出所を特定することで、それが違法な行為によるものかどうかを知ることができる。このような隠し込みの技術は、「データ・ハイディング」と呼ばれている。

図1は、デジタル化されたデータをディスプレイ上に表示した中間調画像である。同図（a）のデジタル化された画像であるメディア・データには同図（b）に示すような「保母」、「川」、「園児」及び「鳥」

といった写真説明（メッセージ）が隠ぺいされている。メディア・データは写真などをもとに画像を細かく分割して、小さな点ごとに明るさや色彩を数値化することにより得られる。その際、画像のもとの数値を意図的に少しだけ変化させておく。数値の変化がごくわずかならば画像の乱れはほとんどないので、人間はその変化にほとんど気がつかない。この性質をうまく利用すると、もとの映像に全く別の情報（メッセージ・データ）を隠し込むことができる。この隠し込まれるメッセージ・データはどのような情報でも構わないが、例えば格子模様、定規のようなもの、または画像の製作者の署名などが挙げられる。メディア・データに隠ぺいされたメッセージ・データは特別なプログラムで処理することにより抽出することができる。従って、この抽出されたメッセージ・データに基づいてメディア・データが改ざんされていないかどうかを調べることができる。

図1（b）に示した各メッセージは画像上の意味のある領域付近に隠ぺいされている。例えば、「鳥」というメッセージは画像中の鳥が存在している領域付近に隠ぺいされ、キャプション（補助的説明）としての役割を果たしている。しかしながら、所有者の情報などといったメッセージを画像中に隠ぺいするためには、そのメッセージは画像中に広く分散させることが好ましい。メッセージの量が多い場合、局所的にメッセージを隠ぺいするとその部分における画質の低下を招くからである。また、画像の一部が切り取られた場合であっても、メッセージが分散されていればそれを抽出できる可能性が高くなるからである。そのために重要なことは、分散され各メッセージ片を隠ぺいする位置をどのようにして決定するかということである。この位置の決定は状態系列Sに基づいて行われる。状態系列Sの各要素を各メッセージに対応付け、この要素に基づき決定された所定位置にそれに対応するメッセージを隠ぺいする

のである。

従来のデータ・ハイディング方法において、状態系列 S は乱数列により決定されていた。図 2 は、従来の方法に基づき画像上に分散されたメッセージ・データの配置を示す概略図である。図 1 (a) に示す画像を

5 I 個の画像領域に分割し、それぞれの画像領域に 0 番目から 9 番目まで順番に番号を付していく。次に、メッセージ・データをメッセージ配列 m で表現し、その配列要素を配列値 $m[n]$ ($0 \leq n \leq 9$) と記述する。各配列値は分割されたメッセージ・データに対応付けられている。状態系列 S 中の要素に基づいて指定される画像上の位置に各メッセージを隠ぺい

10 していく。0 番目のメッセージ $m[0]$ を隠ぺいする位置 p_0 は、以下の式で決定される。

(数式 1)

状態値 $S_0 = \text{初期値 (定数)}$

15 位置 $p_0 = S_0 \bmod I$

上式は、定数を初期値として状態値 S_0 に与えた後にこの状態値 S_0 に対する I (画像領域の数) の剰余が位置 p_0 であることを示している。位置 p_0 の値は、0 から $(I - 1)$ の範囲のいずれかの整数値となる。

20 この整数値を画像領域の順番に対応付けることにより、 i 番目の画像領域にメッセージ $m[0]$ を隠ぺいする。1 番目以降のメッセージ $m[n]$ は、以下の式に基づいてその隠し込む位置 p_n が決定される。

(数式 2)

25 $S_n = R \bmod (S_{n-1})$

$p_n = S_n \bmod I$

この式は、一つ前の状態値 S_{n-1} を乱数の種 (seed) として擬似的な乱数列を発生させ、これを次の状態値 S_n とすることを示している。そして、この状態値 S_n に対する I の剰余を位置 p_n とする。この値に対応する画像領域にメッセージ $m[n]$ を隠ぺいする。

隠ぺいされたメッセージは、状態値 S_0 (初期値) を知っている者のみを読み出すことができる。メッセージを抽出する場合、この初期値に基づき状態値 S_0 に続くすべての状態値 (S_1, \dots, S_g) を計算する。そして状態値に対応した位置を特定し、その位置中に隠ぺいされたメッセージを抽出する。

図 2 から分かるように、 n 番目のメッセージ $m[n]$ を画像上に配置する位置を決めるための状態値 S_n は状態値 S_{n-1} にのみ依存しているので、状態値 S_{n-1} が決まれば状態値 S_n の値も決定される。同様に、状態値 S_{n-1} も状態値 S_{n-2} にのみ依存している。これを再帰的に繰り返すと、状態系列 S のすべての要素 ($S_0, S_1, S_2, \dots, S_g$) を求めることができる。結局、状態系列 S のすべての要素は、最初に初期値として与えた定数のみに依存して決定されることが分かる。そのため、初期値が特定されれば状態系列 S を求めることができるので、分散されているメッセージのすべての位置を特定でき、かつそれらの隠ぺいされているメッセージ内容を抽出することが可能となる。

初期値が第三者に公開されている場合、または初期値を秘密にしていたにも関わらず第三者に知られてしまった場合、この第三者は初期値を用いてメッセージの配置位置を容易に特定できるため、その者がメッセージ・データを消し去さったり、別のメッセージ・データを上書きしたりするおそれが生じる。従来の方法では、第三者が本来の署名を消し去ってその著作物の出所を不明にするといった行為や、本来の署名上に別

の署名を上書きしてあたかもその者が著作者であるように振る舞う行為を有効に防止することが困難であった。

そこで、本発明の目的は、画像や音声といったメディア・データにメッセージ・データを分散して隠し込むための新規な方法を提案することである。また、本発明の別の目的は、第三者がメッセージ・データを改変することが困難なデータ・ハイディング方法を提供することである。

[発明の開示]

上記目的を解決するために、第1の発明は、メディア・データがメディア配列として表現されると共に、メッセージ・データがメッセージ配列として表現されている場合に、メディア配列中の特定の配列要素を指定する状態値 S に基づいて、メッセージ配列の配列要素を分散してメディア配列に隠すデータ・ハイディング方法に関するものである。第1の発明は具体的には次のステップを有している。

15

- (a) j ($j \geq 0$) 番目の状態値 S_j を決定するステップ
- (b) j 番目の状態値と、 j 番目の状態値により指定されるメディア配列の配列要素と、前記メッセージ配列の配列要素とに基づいて、 $(j+1)$ 番目の状態値 S_{j+1} を決定するステップ
- 20 (c) $(j+1)$ 番目の状態値 S_{j+1} が指定する前記メディア配列の配列要素に対して、ハイディング・データを隠すステップ

メッセージ配列が J 個の配列要素を有している場合には、上記のステップ(a)乃至(c)を再帰的に実行することにより、 J 個の配列要素が隠される。ここで、 $j=0$ の場合、つまり最初の状態値 S_0 は、メッセージ配列の配列要素が有するデータに基づいて、決定される。具体的に

25

は、最初の状態値 S_0 を決定する初期関数を用意し、メッセージ配列のすべての配列要素が有するデータに基づく値（例えば、それらのデータの排他的論理和）をこの初期関数の入力とする。そして、初期関数の出力を最初の状態値 S_0 とするのが好ましい。

- 5 上記ステップ(b)において、 $(j+1)$ 番目の状態値 S_{j+1} は、 j 番目の状態値 S_j と、この状態値により指定されるメディア配列の配列要素が有するデータと、メッセージ配列の配列要素が有するデータとの排他的論理和に基づき決定される。具体的には、ハイディング用位置変換関数を用意し、この排他的論理和を位置変換関数の入力とし、位置変換関数の出力を $(j+1)$ 番目の状態値 S_{j+1} とすることが好ましい。例えば、このハイディング用位置変換関数は、公開鍵方式における秘密鍵をパラメータとした暗号化関数とすることができる。上記のハイディング・データは、 j 番目の状態値 S_j により指定されるメディア配列の配列要素とメッセージ配列の配列要素との排他的論理和としてもよい。
- 10
- 15 また、第2の発明は、メッセージ・データがメッセージ配列として表現され、メッセージ・データを含んだハイディング・データがハイディング配列として表現され、かつハイディング・データが分散して隠べいされているメディア・データがメディア配列として表現されている場合、メディア配列中の特定の配列要素を指定する状態値に基づいて、メディア配列からメッセージ配列を抽出するデータ抽出方法に関するものである。この第2の発明は以下のステップを有している。
- 20

- (a) j ($j \geq 1$) 番目の状態値 S_j を決定するステップ
- (b) j 番目の状態値 S_j により指定されるメディア配列の配列要素から、
- 25 ハイディング配列の配列要素を抽出するステップ
- (c) j 番目の状態値 S_j と、抽出されたハイディング配列の配列要素に

基づいて、 $(j-1)$ 番目の状態値 S_{j-1} を決定するステップ

(d) $(j-1)$ 番目の状態値 S_{j-1} が指定するメディア配列の配列要素及び抽出されたハイディング配列の配列要素に基づいて、メッセージ配列の配列要素を抽出するステップ

5

上記ステップ(a)乃至(c)は、抽出終了条件が満たすまで再帰的に実行される。この条件を満たした場合、メッセージ配列のすべての配列要素が抽出されている。上記ステップ(a)において、抽出を開始する際に最初に用いる状態値 S_j は、抽出に必要な情報として抽出者に予め与えられている。例えば、この状態値 S_j は、メッセージ配列を隠ぺいする際に生成された最後の状態値としてもよい。上記ステップ(c)において、

10

$(j-1)$ 番目の状態値 S_{j-1} は、 j 番目の状態値 S_j と、ハイディング配列の配列要素が有するデータとの排他的論理和に基づいて決定される。

このハイディング配列の配列要素は、 j 番目の状態値 S_j により指定さ

15

れるメディア配列の配列要素から抽出される。また、抽出用位置変換関数を予め用意しておき、上記ステップ(c)において、 j 番目の状態値 S_j と、上記のようにして抽出されたハイディング配列の配列要素が有するデータとの排他的論理和を位置変換関数の入力とし、位置変換関数の出力を $(j-1)$ 番目の状態値 S_{j-1} としてもよい。この抽出用位置変換

20

関数は、例えば、公開鍵方式における公開鍵をパラメータとした復号化関数が挙げられる。上記ステップ(b)において、ハイディング配列の配列要素は、 $(j-1)$ 番目の状態値 S_{j-1} により指定されるメディア配列の配列要素とメッセージ配列の配列要素との排他的論理和とする。

また、第3の発明は、メディア・データ中にメッセージ・データを隠ぺいするデータ・ハイディング方法において、(a) メッセージ・データを隠ぺいすべき一のブロック（画像データであればピクセル・ブロック）

25

をメディア・データ中において特定するステップと、(b) 特定された一のブロックの特性値（例えば、画素値、輝度値、分散値等）を求めるステップと、(c) 隠べいすべきデータの内容を、特性値の基準を与える基準値とブロックの特性値との大小関係に対応づけた変換規則を参照して、
5 一のブロックの特性値を操作することによりメッセージ・データを隠べいするステップとを有するデータ・ハイディング方法を提供する。

ここで基準値は、メディア・データ中に存在する他のブロックの特性値により与えてもよい。一のブロック及び他のブロックをメディア・データ中で特定する場合、これらのブロックでペアを構成し、それぞれの
10 ブロックの特性値を求める。そして、それぞれの特性値の大小関係を比較して、変換規則に基づいてペアを構成するそれぞれのブロックの特性値を操作（例えば特性値を入れ替える等）することにより、メッセージ・データを隠べいする。もし、メッセージ・データが多ビットで構成されるならば、上記のステップ(a)乃至(c)を繰り返し実行する。

第4の発明は、メッセージ・データが隠べいされたメディア・データ
15 中からメッセージ・データを抽出するデータ抽出方法において、(a) メッセージ・データが隠べいされている一のブロックをメディア・データ中において特定するステップと、(b) 特定された一のブロックの特性値を求めるステップと、(c) 特性値の基準を与える基準値とブロックの特性値との大小関係を、抽出すべきデータの内容に対応づけた変換規則を
20 参照して、一のブロックの特性値に応じて、隠べいされているメッセージ・データを抽出するステップとを有するデータ抽出方法を提供する。

ここで、基準値はメディア・データ中に存在し、かつ一のブロックとは異なる他のブロックに関する特性値であってもよい。一のブロック及び
25 び他のブロックをメディア・データ中で特定する場合、これらのブロックでペアを構成し、それぞれのブロックの特性値を求める。そして、ペ

アを構成するそれぞれのブロックの特性値の大小関係を、抽出すべきデータの内容に対応づけた変換規則を参照して、それぞれのブロックの特性値に応じて、隠ぺいされているメッセージ・データを抽出する。この変換規則は、一のブロックの特性値が他のブロックの特性値よりも大きい場合、一方のビットを抽出すると規定し、逆の場合には、他方のビットを抽出すると規定している。

第5の発明は、上述のデータ抽出方法を実現するシステムに関する。すなわち、メッセージ・データが隠ぺいされたメディア・データ中から隠ぺいされたメッセージ・データを抽出するデータ抽出システムにおいて、メッセージ・データが隠ぺいされた、アナログ信号としてのメッセージ・データをデジタル信号に変換して、出力する変換手段と、変換手段の出力としてのメディア・データ中において、メッセージ・データが隠ぺいされている一のブロックを特定する特定手段と、特定手段により特定された前記一のブロックの特性値を求める特性値計算手段と、特性値の基準を与える基準値とブロックの特性値との大小関係を、抽出すべきデータの内容に対応づけた変換規則を記憶する記憶手段と、変換規則を参照して、一のブロックの特性値に応じて、隠ぺいされているメッセージ・データを抽出する抽出手段とを有するデータ抽出システムを提供する。

さらに、第6の発明は、上述のデータ抽出システムの機能をワンチップ化した半導体集積回路に関するものである。すなわち、メッセージ・データが隠ぺいされたメディア・データ中からメッセージ・データを抽出する半導体集積回路において、入力信号としてのメディア・データにおいて、メッセージ・データが隠ぺいされているものとして特定された一のブロックに関して特性値を求める手段と、特性値の基準を与える基準値とブロックの特性値との大小関係を、抽出すべきデータの内容に対

応づけた変換規則を参照して、前記一のブロックの特性値に応じて、隠ぺいされているメッセージ・データを抽出する抽出手段とを有する半導体集積回路を提供する。

5 [図面の簡単な説明]

図 1 は、ディジタル化されたデータをディスプレイ上に表示した中間観画像である。

図 2 は、従来に基づき画像上に分散されたメッセージ・データの配置を示す概略図である。

10 図 3 は、メディア配列及びメッセージ配列を説明するための図である。

図 4 は、ハイディング処理の対象となるメディア配列値の関係を示した概略図である。

図 5 は、隠ぺいされる対象を説明した概略図である。

15 図 6 は、メッセージ・データをメディア・データ中に隠ぺいする手順を示したフロー図である。

図 7 は、ハイディングにおける状態値 S_{j-1} と状態値 S_j との関係を示した関係図である。

図 8 は、隠ぺいされたデータからメッセージ・データ抽出する手順を示したフロー図である。

20 図 9 は、抽出における状態値 S_j と状態値 S_{j-1} との関係を示した関係図である。

図 10 は、生成されたメッセージ配列値がメッセージの先頭であるかどうかの判定を説明するための図である。

25 図 11 は、改変等により間違った状態系列 S が生成された状態を示す概念図である。

図 12 は、PBCを用いたデータのハイディング及び抽出を説明するた

めの図である。

図 1 3 は、1 画素をピクセル・ブロックとした場合の P C B によるハイディングを説明するための図である。

5 図 1 4 は、メッセージと位置情報とをオリジナル画像中に隠ぺいすることを説明するための図である。

図 1 5 は、同心円弧を位置情報として用いた場合の図である。

図 1 6 は、位置情報として同心円弧を用いた場合における基準位置 B の特定を説明するための図である。

10 図 1 7 は、同心円弧を位置情報として用いた場合のハイディング及び抽出を説明するための図である。

図 1 8 は、放送システムにおけるブロック図である。

図 1 9 は、インターネットにおける送信側及び受信側のブロック図である。

図 2 0 は、サーバとクライアントのブロック図である

15 図 2 1 は、フィンガー・プリンティング及びウォーター・マーキング用システムのブロック図である。

図 2 2 は、データ抽出システムのブロック図である。

図 2 3 は、データ抽出システムをワンチップ化した半導体集積回路のブロック図である。

20

〔発明を実施するための最良の形態〕

A. データの定義

まず、以下の配列及び系列について定義する。

25 (1) メディア配列：M

(2) メッセージ配列：m

(3) 状態系列: S

(4) 位置系列: p

(1) メディア配列 M

- 5 メディア・データとしては、画像データ、音声データ等が挙げられる。
埋め込まれるデータであるメディア・データをメディア配列 M によって
定義し、その配列要素であるメディア配列値 $M[i]$ を以下のように表現
する。

10 (数式 3)

$M: \{M_0, M_1, \dots, M_I, \dots, M_{I-1}\}$ または、

$M[i] \quad 0 \leq i \leq I-1 \quad I: \text{メディア・データの長さ}$

- 15 例えば、メディア・データが図 1 (a) のような画像の場合、その画
像は図 3 (a) に示すように I 個の画像領域に分割し最初の画像領域を
0 番目のメディア配列値 $M[0]$ とする。i 番目の画像領域がメディア配
列値 $M[i]$ となり、最後の画像領域はメディア配列値 $M[I-1]$ となる。各
メディア配列値が有するデータはその配列値が対応する画像領域の画像
情報である。画像情報は白黒画面ならば濃度であり、カラー画面ならば
20 色の輝度などが挙げられる。画像領域の数が画素数と一致する場合、メ
ディア配列値 $M[i]$ は i 番目の画素の画素値となる。画像領域が例えば
3 × 3 画素というように複数の画素で構成されている場合、画像情報は
それぞれの画素値である。メディア・データが音声の場合、メディア配
列値 $M[i]$ は時間 i における振幅値として定義できる。なお、各配列値
25 $M[i]$ が有するデータは B_M バイトの整数で表現されているものとする。

(2) メッセージ配列 m

メディア・データ中に埋め込まれるメッセージ・データとしては、例えば画像の作成者に関する情報、製造番号、日時、場所等の管理情報、または複写許可に関する情報などが挙げられる。メッセージ・データをメッセージ配列 m によって定義し、その配列要素であるメッセージ配列値 $m[j]$ は以下のように表現する。

(数式 4)

$$m : \{m_0, m_1, \dots, m_j, \dots, m_{J-1}\} \text{ または}$$

$$m[j] \quad 0 \leq j \leq J-1 \quad J : \text{メッセージ・データの長さ}$$

例えば、図 3 (b) に示すように、「DATA HIDING」という 10 文字の英数字がメッセージ・データである場合、 j 番目の英数字をメッセージ配列値 $m[j-1]$ に対応づけ、それが有する内容は対応する英数字を示すデータとする。各配列値 $m[j]$ が有するデータは B_m バイト (英数字の場合には 1 バイト) の整数を表現されているものとする。なおこの場合、メッセージ・データの長さ J は 10 となる。

(3) 状態系列 S

ハイディング処理を行う位置 (メディア配列値) を決定するために状態系列 S を定義し、この系列の要素である状態値 S_j を以下のように表現する。

(数式 5)

$$S : \{S_0, S_1, \dots, S_j\} \text{ または、}$$

$$S_j \quad 0 \leq j \leq J \quad J : \text{メッセージ・データの長さ}$$

この状態系列 S を生成するためのアルゴリズムは本実施例における重

要な点の一つである。状態系列 S の要素数は $(J + 1)$ 個であり、これはメッセージ配列 m の要素数 J よりも 1 個だけ多い点に留意されたい。

(4) 位置系列 p

位置系列 p は、ハイディング処理を行う位置を下式から具体的に特定するためのものである。この位置系列 p の要素である位置 p_j は以下の
5 ように表現される。

(数式 6)

$$\begin{aligned} p : \{ p_0, p_1, \dots, p_J \} \text{ または,} \\ 10 \quad p_j \quad 0 \leq j \leq J \quad J : \text{メッセージ・データの長さ} \\ p_j = S_j \bmod I \end{aligned}$$

位置系列 p は状態系列 S と同数 $(J + 1)$ の要素を有している。位置
系列の要素である位置 p_j は同じインデックス値 j を有する状態値 S_j に
15 対する I の剰余として求められる。従って、位置 p_j が有する値は 0 か
ら $(I - 1)$ の間のいずれかの整数となるので、この値に対応する画像
領域をハイディング処理の対象の領域とする。 I は画像領域の数という
定数なので、状態値 S_j さえ定まれば位置 p_j の値も一意に定まる。従っ
て、ハイディング処理の対象となる位置は実質的に状態系列 S により特
20 定されている。

B. ハイディングのアルゴリズム

本実施例におけるデータ・ハイディング方法は隠ぺいされたデータを
抽出するアルゴリズムと密接な関係を有している。すなわち、隠ぺいさ
25 れたデータを抽出しようとする第三者が所定の情報を有していることを
条件に、メッセージを見ることができる。この場合に重要なことは第三

者がメッセージを抽出する際にその改変を有効に防止することである。
この点に鑑み本発明は以下のような3つの特徴に基づきデータを隠ぺいしている。

- 5 (1) メッセージの特徴に基づいて状態値 S_0 を決定
- (2) メッセージ及び画像データに基づいた状態系列 S の決定
- (3) 隠ぺいの対象となるデータ

(1) メッセージの特徴に基づいて状態 S_0 を決定

- 10 状態系列の最初の要素である状態値 S_0 はメッセージ配列のすべての要素 ($m[0]$ 、 $m[1]$ 、 \dots 、 $m[9]$) の排他的論理和を入力とする初期関数 f_{INI} の出力である。状態値 S_0 及びそれに基づき定まる位置 p_0 は下式で決定される。

- 15 (数式7)

$$S_0 = f_{INI} (m[0] \text{ XOR } m[1] \text{ XOR } m[2] \text{ XOR } \dots \text{ XOR } M[n-1])$$

$$p_0 = S_0 \bmod I$$

- 20 従来の方法では、埋め込むメッセージの内容に関わらず、ある定数を初期値として与えて最初の状態値 S_0 を決定していた。これに対して、この実施例はメッセージの内容、つまりすべてのメッセージ配列値に基づいてこの要素を決定している。図4は画像上にメッセージ・データを分散した状態を示す概略図である。最初の位置 p_0 は最初の状態値 S_0 から特定され図示のような場所になる。

- 25 最初の状態値 S_0 をメッセージ配列 m の特徴から決定している点は本アルゴリズムの特徴の一つである。これにより最初の状態値の与え方を

単に複雑にするためだけではなく、第三者の不正なメッセージの上書きをも有効に防止できる。初期関数 f_{INI} はメッセージの抽出時において終了判定のための関数としても用いられる。これにより第三者が本来のメッセージ以外のメッセージを新たに書き込むことを防止できる。

5 (2) メッセージ及び画像データに基づいた状態系列 S の決定

状態値 S_0 から次の状態値 S_1 を求める。次の状態値は以下の式により特定される。

(数式 8)

10
$$S_1 = SK(S_0 \text{ XOR } m[0] \text{ XOR } M[p_0])$$

すなわち、次の状態値 S_1 は、現在の状態値 S_0 、この状態値が指示するメディア配列値 $M[p_0]$ 及びメッセージ配列値 $m[0]$ の排他的論理和を入力とした関数 SK の出力として決定される。ここでメディア配列値 $M[p_0]$ は状態値 S_0 から計算される位置 p_0 の画像領域のことである。状態値 S_2 以降も同様であり、この関係を一般的に表すと下式のような

15 る。

(数式 9)

20
$$S_{j+1} = SK(S_j \text{ XOR } m[j] \text{ XOR } M[p_j])$$

関数 SK は次の状態値を求めるための位置変換関数であり、現在の状態値、メッセージ配列値及びメディア配列値の排他的論理和をその入力としている。このようにして上記の計算を再帰的に実行することで順次

25 状態値を求めていく。この状態値は $(J+1)$ 個求める必要があるので最後の状態値は S_J となる。図 3 (b) のようにメッセージ配列の要素

数が10ならば、11個の要素数を有する状態値を生成する。このようにして状態系列Sを求めることでハイディング処理の対象となるすべての画像領域を特定する。図4はハイディング処理の対象となるメディア配列値の関係を示している。

- 5 従来の位置系列が最初に与える初期値のみに依存して決定されるのに対し、本アルゴリズムにおける位置系列はメッセージ配列値及びメディア配列値をも考慮して決定されている。第三者が本来のメッセージ上に別のメッセージを上書きしようとした場合、これにより生成される状態系列が異なるので上書きは非常に困難となる。このことは第三者が画像
10 データ自身を改変しようとした場合においても同様である。

(3) 隠べいの対象となるデータ

- 図5は隠べいされる対象を説明した概略図である。前提としてハイディング処理の対象となる位置系列 p が特定されているものとする。まず、位置 p_0 には如何なるデータも隠べいせずに隠べいは位置 p_1 以降の画像
15 領域に施される。具体的には、メディア配列値とメッセージ配列値との排他的論理和結果が隠べいの対象となる。

- まず、位置 p_0 では単にメディア配列値 $M[0]$ のみを取り出す。次に、位置 p_1 における処理として、メッセージ配列値 $m[0]$ と取り出されたメディア配列値 $M[0]$ との排他的論理和を求めてこの結果を位置 p_1 に隠べ
20 いする。この隠べいにより、メディア配列値 $M[p_1]$ の内容が変わる。さらに、位置 p_2 における処理として、メッセージ配列値 $m[1]$ と前の処理により内容が変わったメディア配列値 $M[1]$ との排他的論理和を求め、この結果を位置 p_2 に隠べいする。

- このようなハイディング処理を位置 p_{10} まで実行することでデータの
25 隠べいが完了する。なお、位置 p_{10} に隠べいされる対象はメッセージ配列値 $m[9]$ と前の処理で内容が変更されたメディア配列値 $M[9]$ との排他

的論理和配列である。状態系列 S 及び位置系列 p の要素数をメッセージ配列の要素数よりも 1 つ多く設けたのは、位置 p_0 だけはデータの隠べいが行われないからである。

5 本アルゴリズムにおいて、隠べいされたメッセージを逆に抽出する場合、一番最後のメッセージ配列値 $m[9]$ から逆順で再帰的に抽出する。本アルゴリズムで隠べいされる対象を、メッセージ配列とメディア配列の排他的論理和の結果としたことは、メッセージの抽出手順と密接に係している。従って、この詳細は後述の「メッセージ・データの抽出」の欄において述べる。また、データを実際にハイディングするアルゴリズムに
10 関しては様々な方法が考えられる。第 2 の実施例では、データをハイディングするアルゴリズムの一例として P B C (Pixel Block Coding) という方法について説明する。

C. 第 1 の実施例

15 以下、第 1 の実施例を図 6 の手順に従ってさらに具体的に説明する。図 6 はメッセージ・データをメディア・データ中にハイディングする手順を示したフロー図である。以下の説明においては、適宜、図 4 または図 5 を参照されたい。

初期状態値の計算 (ステップ 100)

20 データの隠べいを行うためには位置系列 p を決定しなければならないが、そのためにまず最初の位置 $p[0]$ を決定する。この最初の位置 $p[0]$ は最初の状態値 S_0 を入力とした初期関数 f_{INI} の出力として決定されるが、この変数 S_0 は以下の式で決定される。

25 (数式 10)

$$S_0 = f_{INI}(m[0], m[1], m[2], \dots, M[J-1])$$

$$= H1 (m[0]//m[1]//m[2]// \cdots //M[J-1])$$

ここでH1はハッシュ関数である。また、演算子「//」はメッセージ配列の各要素をつなげるという意味である。この具体的な演算は、例えば配列要素が有するデータの排他的論理和であってもよい。但し、排他的論理和とした場合にはメッセージ配列値の順序は計算結果に反映されない。つまり、図3(b)の「DATA HIDING」と「TADAH HIDING」とは同じ値となる。そこで例えば、CRC(Cyclic Redundancy Check)という方法を用いればこの順序関係を反映することができる。このアルゴリズムはチェックサムを計算するためのアルゴリズムの一つで、データ列の内容及びデータ列の順序に依存した出力を生成する。

このハッシュ関数H1は、バイト長が B_m バイトである入力(配列値 $m[i]$)に対して、それと異なるバイト長Kの出力(ハッシュ値)を求める関数である。この関数は一方向関数であるから、 $H(x)=y$ においてyからxを推定することは事実上不可能である。

このKバイトのハッシュ値をデータ・ハイディングを実行する際の初期値 S_0 として用いる。ハッシュ値はデータ・ハイディングの際に単に初期値として用いられるものであり、異なる入力に対して異なる出力が事実上保証されていれさえすればよい。従って、ハッシュ値の値自身には特別な意味はない。重要なことは、その演算により配列の特徴を示す値を出力すること、つまり配列要素全体の内容に基づいてハッシュ値が一意に定まりかつその値が配列全体の内容により異なることであるということに留意されたい。

メッセージ・データが図3(b)に示した「DATA HIDING」の場合、すべての英数字を示すデータ(配列値 $m[i]$ が有するデータ)

の排他的論理和に対するハッシュ関数H 1 の出力が状態値 S_0 となる。
この状態値 S_0 に対する I (画像領域の数) の剰余が位置 p_0 となる。これにより初期状態値として状態値 S_0 及び位置 p_0 が得られた。

画素値の抽出 (ステップ 2 0 0)

- 5 ステップ 1 0 0 で得られた位置 p_0 の値に対応する画像領域が有する画像情報を求める。例えば位置 $p_0 = i$ ならばメディア配列値 $M[i]$ である。このデータは B_M バイトの整数で表現されている。

次状態の計算 (ステップ 3 0 0)

- 10 ステップ 1 0 0 で求めた状態値 S_0 の他に、メッセージ配列値 $m[0]$ 及びこの状態値 S_0 から特定されるメディア配列値 $M[p_0]$ から次の状態値 S_1 を決定する。状態値 S_1 は以下の式で求められる。

(数式 1 1)

$$S_1 = SK(S_0 \text{ XOR } m[0] \text{ XOR } M[p_0])$$

- 15 (但し、XORは排他的論理和演算)

- 20 つまり、状態値 S_0 、メッセージ配列値 $m[0]$ 及びメディア配列値 $M[p_0]$ の排他的論理和を求め、この結果を関数 SK の入力とする。そして関数 SK の出力を次の状態値 S_1 としている。このような関数 SK を位置変換関数と呼び、特にメッセージ・データをメディア・データ中に隠し込むための位置変換関数 SK をハイディング用位置変換関数と呼ぶ。なお位置変換関数 SK は隠ぺいされたデータを抽出する抽出用位置変換関数 PK と密接な関係を有するので、この関数の詳細は後の抽出用位置変換関数の説明において詳述する。

- 25 状態値 S_2 以降も同様の手順を実行することで求めることができる。これを一般化すると j 番目の状態値 S_j 及び位置 p_j は以下の式で表現で

きる。

(数式 1 2)

$$S_j = SK(S_{j-1} \text{ XOR } m[j-1] \text{ XOR } M[p_{j-1}])$$

$$p_j = S_j \bmod I$$

(SK: ハイディング用位置変換関数)

ここで、位置 p_j は、前の状態値 S_{j-1} 以外にも、メッセージ・データ及びメディア・データの内容に基づいて決定されている点に再度留意されたい。

ハイディング用位置変換関数 SK の入力として用いられる状態値 S_{j-1} 、メッセージ配列値 $m[j-1]$ 及びメディア配列値 $M[p_{j-1}]$ が有するデータのビット長は、それぞれ K バイト、 B_m バイト、 B_M バイトと異なっている。ビット長が異なる入力に対して排他的論理を計算することはもちろん可能であるが、各入力と同じビット長になるように変換した上で排他的論理和を計算する方が好ましい。すべての入力のバイト長を位置状態が有する K バイトに揃えるために以下の 2 つのハッシュ関数 H 2、H 3 を用いる。

H 2: B_m バイトの整数から K バイトのハッシュ値を生成するハッシュ関数

H 3: B_M バイトの整数から B_m バイトのハッシュ値を生成するハッシュ関数。

すなわち、メッセージ配列値 $m[j-1]$ に対しては、ハッシュ関数 H 2 を用いて、この配列値が有する B_m バイトの整数から K バイトのハッシュ値を生成する。また、メディア配列値 $M[p_{j-1}]$ に対しては配列値が

有する B_m バイトのビット長の整数をハッシュ関数 H_3 を用いて、 B_m バイトのハッシュ値に変換する。そして、さらにハッシュ関数 H_2 を用いることにより K バイトのハッシュ値を生成する。なお、上述した（数式 7）はこのように入力がハッシュ関数で変換されている場合も含めた表現とする。

メッセージの埋め込み（ステップ 400）

メッセージ配列値 $m[j-1]$ とメディア配列値 $M[p_{j-1}]$ との排他的論理を求めてこの結果をハイディング配列値 $Mm[j-1]$ が有するデータとする。ステップ 300 で求められた位置 p_j にはこのハイディング配列値 $Mm[j-1]$ が有するデータが隠ぺいされる。ここでハイディング配列値 $Mm[j-1]$ とは、ハイディング配列 Mm の配列要素であって次式のように定義される。

（数式 13）

$$Mm : \{ Mm[0], Mm[1], \dots, Mm[j], \dots, Mm[J-1] \}$$

$$Mm[j] = m[j] \text{ XOR } M[p_j]$$

ここで重要なことは、隠ぺいされるデータはメッセージ配列値 $m[j]$ 自身ではなく、メッセージ配列値 $m[j]$ とメディア配列値 $M[p_j]$ との排他的論理和により生成されるハイディング配列値 $Mm[j]$ であるということである。ハイディング配列値 $Mm[j-1]$ は、関数 X によって位置 p_j に隠ぺいされる。これにより、メディア配列値 $M[p_j]$ の有するデータが変化する。内容が変化したメディア配列値 $M[p_j]$ を $M'[p_j]$ で表す。なお、関数 X の具体的な内容、つまりハイディング配列を所定の位置にどのようにして隠ぺいするかというアルゴリズムについては、その一例である PBC を第 2 の実施例において説明する。

判断 (ステップ 500)

- 5 j の値が J (メッセージ配列の要素数より 1 大きい値) と等しいかどうかを判断する。 j が J に等しいということはすべてのメッセージ配列値の隠べいが完了したことを意味する。 j の値が J に満たない場合は、
 j に 1 を加えてステップ 200 に戻り j の値が J になるまでステップ
 200 から 400 を再帰的に実行する。このようにして下式で表される
 $(J + 1)$ 個の要素を有する状態系列 S 及び位置系列を得ることができる。

10 (数式 14)

状態系列 $S : \{S_0, S_1, S_2, \dots, S_J\}$

位置系列 $P : \{p_0, p_1, p_2, \dots, p_J\}$

- 15 また、メディア配列 M はデータが隠べいされることによりその要素は
 以下のように変化する。

(数式 15)

(ハイディング前のメディア配列)

$M : \{M[0], \dots, M[p_0], \dots, M[p_1], \dots, M[p_{I-1}]\}$

20 (ハイディング後のメディア配列)

$M' : \{M'[0], \dots, M'[p_0], \dots, M'[p_1], \dots, M'[p_{I-1}]\} =$
 $\{M[0], \dots, M[p_0], \dots, M'[p_1], \dots, M'[p_{I-1}]\}$

- 25 M' はハイディング後のメディア配列を意味し、また $M'[1]$ はハイ
 ディング前のメディア配列値の内容が変化したことを示す。つまりメ
 ディア配列 M' は本来のメッセージ配列 M の要素の内の状態系列 S で特定

される J 個の配列要素の内容のみが変化したことを意味している。なお、状態値₀に対応する配列要素 $M[p_0]$ は、データ内容が変化しないので、 $M'[p_0]$ は $M[p_0]$ に等しい。

図 7 は、ハイディングにおける状態値 S_{j-1} と状態値 S_j との関係を示した関係図である。次の状態値 S_j は、状態値 S_{j-1} 及びハイディング配列 $Mm[j-1]$ ($M'[p_{j-1}] \text{ XOR } m[j-1]$) の排他的論理和を計算し、この計算結果を位置変換関数 SK の入力とすることによって求められる。メディア配列値 $M'[p_{j-1}]$ は前状態のハイディングで既にその内容が変化している。また隠ぺい対象であるハイディング配列値 $Mm[p_{j-1}]$ は、関数 X により位置 p_j に隠ぺいされる。これによりその位置のデータ $M[p_j]$ が変わる。

状態値の抽出 (ステップ 6 0 0)

最終的に、以下の 2 つの情報を抽出することにより、メッセージの隠ぺいは終了する。

- (1) ハイディング後のメディア配列 M'
- (2) 最終状態値 S_j

メディア配列 M' はステップ 4 0 0 でデータをメディア・データ中に隠ぺいすることで最終的に得られた配列である。また最終状態値 S_j は最後に計算された J 番目の状態値である。これらの情報は以下に説明するメッセージ・データを抽出する際に必要となる。なお、隠ぺいされたメッセージを抽出する際には、最後、すなわち J 番目の状態値のみを抽出者が知っていれば、 $(J-1)$ 番目以前の状態値 (S_0 乃至 S_{j-1}) を直接知っている必要はない。これらの状態値は最終状態値を逆変換することで再帰的に特定できるからである。もちろんこの抽出者は後述する

必要な情報を有していることが条件である。

(メッセージ・データの抽出)

5 メッセージ・データの抽出を実行するために第三者に与えられる情報は、以下の3つである。

(1) ハイディング後のメディア配列 M'

(2) 最終状態値 S_J

(3) 抽出用位置変換関数 P_K

10

情報(1)及び情報(2)は、上述の通りメッセージ・データを埋め込む際に最終的に生成された情報である。ここで情報(3)の抽出用位置変換関数 P_K についてハイディング用位置変換関数との関係を考慮しつつ説明する。

15

a. ハイディング用位置変換関数 S_K 、抽出用位置変換関数 P_K

20

メッセージを隠ぺいする際に次の状態値を生成する関数をハイディング用位置変換関数 S_K を定義したように、メッセージを抽出する際においても前の状態値を生成する関数を抽出用位置変換関数 P_K を定義する。ハイディング用位置変換関数 S_K と抽出用位置変換関数 P_K は、以下の式に示すように逆関数の関係が成立する。

(数式 16)

$$P_K(S_K(x)) = x$$

$$S_K(P_K(x)) = x$$

25

従って、メッセージ配列 m をハイディング用位置変換関数 S_K を用い

て変換した結果に対して、その逆関数 P_K でさらに変換すれば最初のメッセージ配列 m を抽出することができる。

上記の式を満たすような関数は様々な関数が考えられる。しかしながら、第三者が与えられた抽出用位置変換関数 P_K からハイディング用位置変換関数 S_K を再現することを事実上不可能にするために、この関数として公開暗号方式における暗号化関数及び復号化関数を用いていることが好ましい。公開鍵方式のアルゴリズムはいくつかの方式が存在するがそのどれを用いてもよい。一例として典型的な方式である RSA 方式について説明する。RSA 方式のアルゴリズムは、以下の通りである。

1. 2つの大きな素数 p, q を選び、 $n=p*q$ を計算する。
2. $r=\text{lcm}(p-1, q-1)$ を計算し、 $\text{gcd}(d, r)=1$ になるように d を選ぶ。
3. $e*d=1 \pmod{r}$ 、 $0 < e < r$ となるように e を決定する。
4. e を公開鍵として公開し、 n も公開する。 d は秘密鍵として秘密にしておく。
5. あるメッセージ m の暗号化は、 $m^e = c \pmod{n}$ を満たすような c を計算し、この c が暗号化されたメッセージとなる。
6. 暗号化されたメッセージの復号化は、 $c^d = m \pmod{n}$ を満たすような m を計算し、この m が復号化されたメッセージとなる。

このアルゴリズムを本実施例に適用すると、ハイディング用関数 S_K 及び抽出用関数 P_K は以下のようになる。

(数式 17)

$$S_K(m) = x^d \pmod{n}$$

$$P_K(m) = x^e \pmod{n}$$

すなわち、画像の作成者である発行者は秘密鍵 d を保有しこれを用いてハイディング用関数 SK を得る。この関数 SK を用いてメッセージ・データを埋め込むための位置状態系列 S を生成し、メッセージ・データをメディア・データ中に埋め込む。配布されたこのデータを受け取った第三者は公開鍵 e を用いて抽出用関数 PK を得る。この関数 PK を用いて上記の位置状態系列 S を再生して、メッセージを読む。公開鍵方式において、公開鍵は第三者に公開されているが、秘密鍵は画像などを制作した著作者のみが保有しているので第三者はその内容を知ることはできない。従ってハイディング用位置変換関数の内容を第三者が知ることはできない。公開鍵から秘密鍵を計算することはそのための計算量が膨大になるので、第三者がハイディング用位置変換関数 SK を知ることは事実上不可能である。従って第三者がオリジナルのデータを改変することを有効に防止することができる。

メッセージを抽出する手順を説明するために必要となる排他的論理和の重要な性質について簡単に説明しておく。排他的論理和演算には以下のような性質がある。すなわち A と B との排他的論理和に対して、さらに B との排他的論理和を求めると A が再現されるということである。

(数式 18)

$$(A \text{ XOR } B) \text{ XOR } B = A$$

(抽出のアルゴリズム)

図 8 は、埋め込まれたメッセージ・データを抽出する手順を示したフロー図である。

初期状態値の計算 (ステップ 110)

まず、抽出者に与えられている情報である最終状態値 S_J から、次式に従ってメッセージ配列値 $m[J-1]$ が隠し込まれている位置 p_J を求める。

5 (数式 19)

$$p_J = S_J \bmod I$$

ハイディング値の抽出 (ステップ 120)

位置 p_J に対応するメディア配列 $M'[p_J]$ はその領域の本来の画像
 10 情報中にハイディング配列値 $Mm[J-1]$ が隠べいされている。この配列
 $Mm[J-1]$ はメディア配列値 $M'[p_{J-1}]$ 及びメッセージ値配列 $m[J-1]$ の
 排他的論理和として求められたものである。そこでメディア配列値 M'
 $[p_J]$ からハイディング配列値 $Mm[J-1]$ を抽出するために関数 X' を
 定義する。次式のような関数 X' の具体的な内容は第 2 の実施例におい
 15 てその一例を説明する。

(数式 20)

$$Mm[J-1] = \text{関数 } X' (M'[p_J])$$

20 前状態の計算 (ステップ 130)

次に、状態値 S_J 及び上記の関数 X' から求められたハイディング配
 列値 $Mm[J-1]$ の排他的論理和を計算することで 1 つ前の状態値 S_{J-1} を
 求める。ここでは上述の排他的論理和の数学的性質を利用している点に
 留意されたい。

25

(数式 21)

$$\begin{aligned}
 & PK(S_J) \text{ XOR } X'(M'[p_J]) \\
 &= (S_{J-1} \text{ XOR } Mm[J-1]) \text{ XOR } Mm[J-1] \\
 &= S_{J-1}
 \end{aligned}$$

- 5 すなわち、抽出用位置変換関数 PK はハイディング用位置変換関数の逆関数なので、この関数を用いれば状態値 S_J から状態値 S_{J-1} とハイディング配列値 $Mm[J-1]$ との排他的論理和の結果を再現できる。この結果とステップ 120 で求められたハイディング配列値 $Mm[J-1]$ との排他的論理和を求めることにより、1 つ前の状態値 S_{J-1} を特定できる。

10 メッセージの計算 (ステップ 140)

状態値 S_{J-1} が求まればこれに対応するメディア配列値 $M'[p_{J-1}]$ が特定されるので、メッセージ配列値 $m[J-1]$ を次式により抽出することができる。図 3 (b) のメッセージが隠ぺいされていたならば、このステップにより最後尾の英数字「G」が抽出される。

15

(数式 22)

$$\begin{aligned}
 & M'[p_{J-1}] \text{ XOR } Mm[J-1] \\
 &= M'[p_{J-1}] \text{ XOR } (M'[p_{J-1}] \text{ XOR } m[J-1]) \\
 &= m[J-1]
 \end{aligned}$$

20

状態値及びメッセージ配列値の抽出をインデックス値 j ($1 \leq j \leq J$) を用いて一般的に表現すると次式のようなになる。

(数式 23)

25

$$\begin{aligned}
 & S_{j-1} : \\
 & PK(S_j) \text{ XOR } X'(M'[p_j])
 \end{aligned}$$

$$= (S_{j-1} \text{ XOR } Mm[j-1]) \text{ XOR } Mm[j-1]$$

$$= S_{j-1}$$

$m[j-1]$:

$$M'[p_{j-1}] \text{ XOR } Mm[j-1]$$

$$5 \quad = M'[p_{j-1}] \text{ XOR } (M'[p_{j-1}] \text{ XOR } m[j-1])$$

$$= m[j-1]$$

上記の式が示すデータ関係を示したのが図9である。抽出における状態値 S_j と状態値 S_{j-1} との関係を示した関係図である。図7と対比してみると抽出の手順はハイディングの手順をと逆に実行していることがわかる。

判断 (ステップ150)

メッセージ配列値 $m[j]$ が生成されることにそれが配列値がメッセージ配列の先頭なのかを判断する。先頭であると判断された場合、メッセージ配列 m のすべての要素を抽出できたことになる。メッセージ配列 m は最後の要素から逆順で抽出されるので、図3(b)の例では「GNIDIHATAD」という順序でメッセージが抽出される。これをステップ160でメッセージを逆の順序で並び替えることにより完全なメッセージが生成される。先頭でない場合、ステップ120からステップ140を先頭と判断されるまで再帰的に実行する。

メッセージ配列 m のある要素が先頭か否かの判断は、生成された状態値 S_j とハッシュ関数 $H1$ との出力が一致するかどうかである。ハッシュ関数 $H1$ には、状態値 S_j においてそれまでに生成されたメッセージ配列 m のすべての要素の排他的論理和を入力する。逆順に生成されたある状態値 S_j がハッシュ関数 $H1$ の出力とが次式に示すような関係ならば、この j の値が0である(数10参照)。

(数式 2 4)

$$S_j = f(m[j-1] \text{ XOR } m[j-2] \text{ XOR } \cdots \text{ XOR } m[j]) = S_0$$

- 5 上式の関係が成り立つのは $j = 0$ の場合のみで、それ以外 ($j \neq 0$) の場合にはこの関係は成立しない。従って最終状態値 S_j が状態値 S_j が逆順に生成される度に、この状態値 S_j 及び抽出されたすべてのメッセージ配列値に基づいたハッシュ関数の出力の一致を比較していく。図 10 は、生成されたメッセージ配列値がメッセージの先頭であるかどうかの判定を説明するための図である。まず最終状態値 S_j から一つ前の状態値 S_{j-1} を求めると共に、メッセージ配列値 m_{j-1} を求める。この配列値を入力とした初期関数 f の出力 F は状態値 S_{j-1} とは一致しない。求められた状態値が S_0 ならば、この値は初期関数の出力 F と一致するので先頭と判断できる。このように本アルゴリズムは次のような 2 つの特徴があるので、第三者によるメッセージの改変を防止する上で非常に重要である。
- 10
- 15

(1) 別メッセージの上書き防止

- 従来技術では、発生する位置系列 S はメッセージの内容に関わらず最初に与える定数にのみ依存していた。第三者はその定数さえ分かればメッセージを消去したり本来のメッセージが存在する位置に新たな別内容のメッセージを上書きすることが可能であった。これに対して、本アルゴリズムでは位置系列はメッセージの内容にも依存して生成されるため、メッセージが異なれば発生する異なる位置系列が生成される。隠ぺいされる位置は位置系列に基づいているので、本来のメッセージが存在している位置に内容の異なる別のメッセージを隠ぺいすることはできない。
- 20
- 25
- これはメディア・データについても同様である。

(2) 別メッセージのハイディング防止

本アルゴリズムでは、抽出の終了を判断するために数 2 4 に示す条件を判断している。この条件を満たすのは、抽出されるメッセージの内容が本来のメッセージと同じで、かつメッセージ・データの長さ (J) と等しい長さのメッセージが抽出された場合のみである。この要件を満たさない限り抽出は決して終了しない。従って、最終状態値 S_J に基づいて逆順で本来のメッセージ以外のデータを隠べいしようとした場合には、決して数 2 4 の要件を満足することはないので永久に計算が終了しない。従って本来のメッセージが存在する場所以外の場所にメッセージを隠べいしようとしても、計算が終了しないので実質的に隠べいできない。

図 1 0 及び図 1 1 に示すように第三者がメッセージ配列値を改変した場合には、改変されたメッセージに基づいて異なった状態系列 S' が生成される。従って、状態系列 S' より特定される位置以外の位置にある本来のメッセージを消去したり上書きしたりすることはできない。図 1 1 に示すような改変により生じた状態系列 S' においては決して抽出が終了したと認定されることはない。事実上他のメッセージを書くことができないので、第三者の改変を有効に防止することができる。

D. 第 2 の実施例

ここでは、隠べいの対象となるデータのあるあるメディア・データ中に埋め込む方法及び逆に埋め込まれたデータを抽出する方法の一つであるピクセル・ブロック・コーディング (Pixel Block Coding) (以下、PBC という) について説明する。PBC を用いた場合、データをハイディング及び抽出は以下の述べるような変換規則に従って処理される。

(基本アルゴリズム)

一般的に、隣接した 2 つの画素の画素値等の 1 次特性は互いに高い相

関関係を有している。従って画素値を入れ変えたとしても、画像が視覚的に認識できる程度の劣化は生じない。この性質に鑑みて、本アルゴリズムは少なくとも1つの画素を有する画像領域をピクセル・ブロックとして定義し、ある変換規則に基づき意図的に隣接したピクセル・ブロックの特性値を入れ替えることで、1ビットのデータを隠ぺいする。すなわち、データは、隣接するピクセル・ブロックの特性値の入れ替えにより表現される。またデータの抽出時には、この変換規則に基づき決定される抽出規則に従ってデータを抽出する。

ビット情報は隣接した2つのピクセル・ブロックの特性値（例えば、輝度値）を以下の変換規則に従って入れ替えること表現される。

ビット・オン <1>: 一方のピクセル・ブロック ($P B_1$) の特性値が他方 ($P B_2$) の特性値より大きい場合
ビット・オフ <0>: 一方のピクセル・ブロック ($P B_1$) の特性値が他方 ($P B_2$) の特性値より小さい場合

またビット情報は、以下の抽出規則に従って隣接した2つのピクセル・ブロックの特性値（例えば、輝度値）を比較することにより抽出される。

一方のピクセル・ブロック ($P B_1$) の特性値が他方 ($P B_2$) の特性値より大きい場合: ビット・オン <1>
一方のピクセル・ブロック ($P B_1$) の特性値が他方 ($P B_2$) の特性値より小さい場合: ビット・オフ <0>

25

図12は、PBCを用いたデータのハイディング及び抽出を説明する

ための図である。ピクセル・ブロック $P B_1$ 、 $P B_2$ は例えば 3×3 画素のように複数の画素の集合として定義してもよいし、1 画素を 1 ピクセル・ブロックと定義することも可能である。隣接するピクセル・ブロックは高い相関を有しているので、それらの位置を入れ替えたとしても画像が視覚的に認識できる程度に劣化したとは感じることはないであろう
5 (図 12 (a))。

オリジナル画像におけるピクセル・ブロックの位置が同図 (b) である場合を考える。まず二つのピクセル・ブロックの特性値を比較し、その結果、 $P B_1$ の特性値の方が $P B_2$ の特性値よりも大きい場合を考える。
10 オリジナルにデータ "1" を隠べいする場合、ピクセル・ブロックの特性値が変換規則におけるデータ "1" の条件を既に満たしているので、これらのブロックの特性値の入れ替え行われな。データを抽出する際、 $P B_1$ の特性値が大きい場合はデータ "1" であると抽出規則が定めているので、データ "1" が抽出される。

一方、オリジナルにデータ "0" を隠べいする場合、オリジナルにおけるピクセル・ブロックの特性値の関係は変換規則におけるデータ "0" の条件を満たさないので、ピクセル・ブロックの特性値を入れ替える。
15 しかしながらこの入れ替えは視覚的には認識できない。抽出時は、抽出規則に従ってこれらのブロックの特性値の関係からデータ "0" が抽出
20 される。

このように P B C では、隠べいの対象となる情報を隠べいするのに十分な数のピクセル・ブロックを画像中から選択する。そして選択された一のピクセル・ブロックとそれに隣接するピクセル・ブロックのペアを作ることにより、このペアの列を生成する。このようにして列の先頭から
25 順々に隠べい対象となるビットを隠べいしていく。

この列は第 1 の実施例における状態系列 S に対応付けてもよい。例え

ばピクセル・ブロックを第1の実施例におけるメディア配列Mの配列要素Mに対応付ける。ハイディング作業において逐次的に生成された状態系列の各配列要素（状態値 S_j ）及びそれに隣接するメディア配列値とでペアを作る。そしてこのペアに対して上記処理を施すことが考えられる。またある乱数の種（シード）から発生される疑似乱数列をもとに決定することももちろん可能である。

抽出時には、ハイディング時と同じブロック列をスキャンする。それぞれのペアがビット・オンを表すかオフを表すかを抽出規則に従って1ビットずつ集めることで全体のメッセージを抽出する。もしペアであるピクセル・ブロックの特性値が同じであるならば、そのペアはハイディング時と同様にスキップする。ブロック列あるいはその列生成方法を秘密にすれば、隠べいされた情報を他人から隠すことができる。

なお、PBCにおいて、埋め込み位置は、画質及び抽出精度に鑑みて決定するのが好ましい。すなわち埋め込み対象となっているペアを構成するピクセル・ブロックの特性値の差があまり大きいと、入れ替え操作により画質が劣化するおそれがある。このような画質の劣化を抑制するために、第1の閾値（上限）を設けておき、特性値の差がその閾値以上であればそのペアにはビットを埋め込まないようにすることが好ましい。

また、特性値の差が小さければ入れ替え操作による画質の劣化はほとんど生じないが、逆にノイズの影響により大小関係が反転してしまい、抽出時に埋め込まれたビットが抽出できないおそれがある。従って抽出精度の低下を抑制するためには、第2の閾値（下限）を設けておき、特性値の差がその閾値以下であればそのペアにはビットを埋め込まないようにすることが好ましい。

これらのケースに該当するペアには何も操作を施すことなくスキップ

する。そして隠べいすべきビット情報を先送りして、次のペアを対象に隠べいする。

(ブロックの特性値)

5 特性値としてピクセル・ブロックの1次特性に関する値及び2次特性に関する値を用いることができる。1次特性はピクセル・ブロックの輝度や色度のように画素値の直接的なパラメータである。また2次特性は、前記パラメータの平均値や分散といった統計的な性質を示す値のように、1次特性をを分解することで得られる。さらに特性値は複数の画素値からなる配列と所定の配列(マスク)との演算結果としてもよく、周波数
10 変換を行うことにより得られる特定の要素値とすることも可能である。一般に、1次特性は隣接する2つのピクセル・ブロックにおいて高い相関関係を有している。これに対して2次特性は隣接しない離れた二つのブロックにおいて高い相関関係を有し得る。従ってPBCの対象となるピクセル・ブロックは必ずしも隣接するブロックに限定されない点に留意されたい。以下、ピクセル・ブロックの特性値として1次特性である
15 輝度値を、また2次特性である分散値を例に説明する。

まず、ピクセル・ブロックの特性値を輝度値とする場合について説明する。1画素をピクセル・ブロックに対応付けた場合、このブロックの特性値として画素の輝度値をそのまま使うことができる。自然画像では
20 大抵の場合、隣接する画素の相関は非常に高いため、それらを入れ替えても大きな画質の劣化にはならない。図13は1画素をピクセル・ブロックとした場合のPCBによるハイディングを説明するための図である。

次に、特性値を分散値とする場合について説明する。 $n \times m$ 画素でピ
25 クセル・ブロックを構成するような場合、ピクセルの輝度値をブロック間で入れ替えると、画像上に縞模様が生じるなど画質に大きな劣化が生

じる。従ってピクセル値をそのままブロックの特性値として使うことは好ましくない。そこでピクセル輝度の分散値を特性値として用いる方法が考えられる。

5 ピクセル・ブロックの輝度値の性質を平均値 h と分散値 d とに分解したとき、隣接するピクセル・ブロックで平均値 h はそのまま分散値 d のみを入れ換えたとしても画質に与える影響は少ないということが知られている。そこでこの性質を生かしてピクセル・ブロックの特性値をこの分散値 d とし、これを変換規則に従って入れ替えることでデータを隠

10 図 1 2 (c) のようにピクセル・ブロック $P B_1$ が、平均値 h_1 、分散値 d_1 を有し、ブロック $P B_2$ が平均値 h_2 、分散値 d_2 を有する場合を考える。ビット "1" を隠ぺいする場合、 $d_1 < d_2$ なので変換規則におけるビット "1" の条件を満たさない。そこで両ピクセル・ブロックの分散値 d のみを入れ替える。これは、二つのピクセル・ブロック間において、その平均値 h は変更せずに分布の山の形だけ交換することに相当する。

(ハイディングできる情報量)

15 P B C においてハイディングできる情報量は画像サイズとピクセル・ブロックのサイズによってその上限は以下のように決定される。

20

(画像サイズ) / (ピクセル・ブロックのサイズ) / 2 [bit]

25 例えば 384x256 サイズの画像に 1x1 サイズのピクセル・ブロックを適用する場合、ハイディングできる情報量は 6 K バイトが上限である。但し、比較する特性値が同一である場合のようにすべてのピクセル・ブロックが隠ぺいのために使えるとは限らないので、実際にはこの情報量より小

さくなる。また隠ぺいは可能であっても、画質の劣化を抑えるために交換処理を施さない場合もあるので、情報量はさらに小さくなることもある。

(画質保存・劣化)

5 画像上で、例えばエッジ特徴にまたがる二つの隣接画素では、その輝度値が大きく異なる値を取ることが知られている。従って、この二つを入れ換えるとエッジ特徴を壊すことになり、視覚的にも画像の劣化が大きく見える。そこで画質の劣化を抑えるために交換する輝度値の差にある閾値を設けておく。そしてその閾値を越えた場合には、特性値の入れ
10 替えを行わずに先送りして、そのペアをスキップする方法が有効である。閾値は画像データから計算される分散値をもとに決定することもできるし、またブロック周辺の局所的な分散値をもとに決定してもよい。

分散値がゼロに近い小さなブロックと、ゼロから遠い大きなブロック
15 とで分散値を交換すると、小さなブロックでの変化が大きくなり視覚的に画質が劣化したことが分かってしまう。従って分散値の小さい方で閾値と比較して、それを下回れば入れ替えを行わないようにしてもよい。

(PBCの耐性)

隣接するピクセル・ブロックの特性値を比較しブロックの特性値を入れ替えることに対応づけたデータの隠ぺいをしているため、その二つの
20 ブロックの相対的な関係が保たれている限り、隠ぺいされた情報を正しく取り出すことができる。従って、色合い調整やγ補正を施した場合であっても特性値の大小比較に基づいて隠ぺいされた情報は保存されることが期待される。また、上述の分散値を交換する方法において、特にピクセル・ブロックを8×8サイズにした場合には、J P E Gによる圧縮
25 処理を施した後でも十分な精度で隠ぺいされた情報を抽出することが可能である。我々の実験によれば、ファイルサイズが5%になるように”

損失あり圧縮”を施した場合でも、情報量は90%の保存率であった。
分散値交換法では、印刷／スキャン操作など、D／AおよびA／D変換
を経た場合でも、隠ぺいされた情報を有効に保存できることと思われる。

5 (PBCの拡張)

なお、上記のPBCは一例であって、それ以外にも様々な方法が考
えられる点に特に留意されたい。上記の実施例から分かるとおり、デー
タの埋め込み及び抽出のためには、特性値の大小関係を規定した規則に従
ったピクセル・ブロックの特性値の操作が重要である。その意味で、上
10 記のように特性値を入れ替える場合以外にも、一方の特性値に所定値を
加算したり、または他方の特性値から所定値を減算すること（さらには
これら両方の操作を行ってもよい）により、規定された大小関係を満た
す操作も可能である。この場合、この所定値は一定の値であってもよい
が、処理対象となるピクセル・ブロックの状態に応じて、その値を適応
15 的に変化させるようにしてもよい。また、PBCの拡張として、特性値
の符号を2値情報に対応づけた規則を定義し、この規則に従って、デー
タを埋め込み及び抽出することも可能である。

本発明の本質は、意味のある規則に従って、ある基準値（例えば一方
のピクセル・ブロック）に対して画像データ中の他のピクセル・ブロッ
クの特性値を操作する点にある。すなわち、特性値の基準を与える基準
20 値をピクセル・ブロックの特性値との大小関係に対応づけた変換規則を
参照して、一のピクセル・ブロックの特性値を操作することによりデー
タを隠ぺいする。その意味で、本発明は特性値を操作する明確な基準が
与えられさえすればよく、その基準が画像データ中の所定領域（ピクセ
ル・ブロック）である必要は必ずしもない。従って、その基準を画像デ
25 ータ以外のデータで与えてもよい。例えば、所定値（基準値）が配列さ

れた、ピクセル・ブロックと同じ大きさを有する固定的なマスク・パターンを特性値操作の基準として用いてもよい。この場合、データの隠ぺいの際には、特定されたあるピクセル・ブロックの特性値を、マスク・パターン中の基準値との大小関係で操作すればよいし、抽出時には、その大小関係に応じてデータを抽出することができる。

E. 第3の実施例

ここでは基準位置に関する情報をハイディングする方法について説明する。上記のようなデータ・ハイディング技術は、原画像からピクセル・ブロックを選択して処理を施し抽出時には処理されたピクセル・ブロックからメッセージを抽出している。従ってメッセージを抽出するためにはそのピクセル・ブロックの位置情報は不可欠である。ピクセル・ブロックの位置は、画像のある領域（第1の実施例ではオリジナル画像の左上の位置）を基準として、この位置情報に基づいて相対的な位置が特定されている。ところが画像の一部を切り出す等の画像の編集作業を第三者が行うと、画像の基準位置を特定できなくなるために、メッセージの抽出に失敗してしまう可能性が生じる。再び図3（a）に基づいて説明すると、オリジナル画像中の一部（図中のは破線領域）が切り出されてしまった場合、この切り出された画面からは本来の基準位置（メッセージ配列の0番目の配列要素の位置M[0]）が分からない。

データ・ハイディングに対する重要な要求事項は、隠ぺいされた情報が第三者により除去しにくいこと、または第三者が悪意にデータを改変した場合や、J P E Gのような損失のある画像圧縮が施された場合においても、隠ぺいされた情報を正しく取り出せることである。そこで、図14に示すようにメッセージの他にさらに基準位置を特定するための情報もオリジナル画像中に隠ぺいすることが好ましい。このような位置情報を隠ぺいしておくことで、改変・圧縮された画像からでもメッセージ

を正しく抽出することが可能となるからである。そこで、メッセージ・データ中にメッセージ・データの他にメディア・データの基準位置を特定するための情報をも隠べいしておく。この基準位置に関する情報はメッセージ・データ全体に隠べいされている。メッセージ・データの一部分が切り取られた場合においても、切り取られた部分的なメッセージ・データから本来のメッセージ・データの基準位置またはこの基準位置からの相対的な位置を検出できる情報である。例えば、以下に述べるように基準位置を中心とした同心円弧を画像全体に隠べいしておいてもよい。

10 (同心円弧を位置情報とした場合)

位置情報として図15に示すような同心円の弧を用いる。この同心円弧はオリジナル画像の左上の点(基準位置)を中心とし所定の間隔で描かれている。切り出された部分画像から基準位置を正しく抽出するためには、切り出されるであろうと想定される部分画像中に少なくとも一本の円弧が含まれていることが必要である。従って同心円の間隔はその上な状況を想定して設定される。

基準位置は、「円周上の点を中心にしてその円と同じ半径で円を描いた場合、描かれた円周は必ずもとの円の中心点を通る」、という円の性質を利用して特定することができる。図16は位置情報として同心円弧を用いた場合における基準位置Bの特定を説明するための図である。まず、切り出された部分画像中に存在する3つの同心円弧(C_1 、 C_2 、 C_3)上にそれぞれ存在する任意の3点(a_1 、 a_2 、 a_3)を特定する。次にそれぞれの点から異なる半径(r_1 、 r_2 、 r_3 、 r_4 、...)の円を描く。この場合、上記の円の性質から、円が交わってできる交点のうち交わっている円の数が多い交点Bを基準位置として認定する。デジタル画像の場合、ピクセルが格子状に離散的に配置されているので、上

記のような円を描いていけば1ピクセルもずれることなく基準位置を特定することができる。

なお、左上の点（基準位置）から離れた円（半径の大きな円）については、部分画像が2本以上の円弧を含むように円弧の間隔を狭めてもよい。円弧は半径が大きくなるに従って直線要素を多く含むようになるため、基準位置の算出値に幅が生じやすくなる。間隔を狭めておけば部分画像中が多くの円弧を含むのでそのような幅を小さくできる。なお、基準位置を同心円の中心を左上及び右下の両方にとっておけば、2つの中心点からオリジナル画像のサイズを求めることができる。

（同心円弧のハイディング）

図17は、同心円弧を位置情報として用いた場合のハイディング及び抽出を説明するための図である。同図（a）は、オリジナル画像中に第2の実施例に示したような方法を使ったメッセージの隠ぺいを施し、その後に位置情報としての同心円弧をさらに隠ぺいしている。同心円弧の位置情報は隠ぺいされた画像情報のLBPをのピクセルを使って隠ぺいされる。例えば同心円弧上のピクセルのLBPを"1"に設定する。LBPを用いる理由はその値を変更しても画像は視覚的にほとんど変化しないからである。また同図（b）は、オリジナル画像にまず位置情報を隠ぺいし、その後にメッセージをさらに隠ぺいしている。

（同心円弧の抽出）

2次元の投票配列Tを作成する。配列のサイズは切り出されるであろうと想定される部分画像がどの程度の大きさまでであるかという点を考慮して決定される例えば配列の幅を $(2m-1)$ とすれば、オリジナルの画像の $1/m$ 倍の大きさの部分画像にまで対応することができる。投票配列Tの各要素は基準位置Bの候補であり要素の値はその得票数を示す。ここで対象となる部分画像が投票配列の中心に位置するように両者

の座標を対応付けておく。

部分画像をスキャンしていき、LBPが"1"である部分に出会った
らその点を中心にして投票配列上の既知の半径すべてについて円弧を描
く。そして投票配列Tの各要素の得票数を1増やす。このとき、各要素
5 に対応する点が隠べいされている円周上の点であれば、ここで描いた円
弧の内少なくとも1つは必ずもとの中心点を通っている。

スキャンを部分画像の縦横交互に実行して、LBPが"1"に出会う
ごとに上記手順を行う。これにより得票数の一番多い要素に対応する位
置が基準位置Bと認定される。一般に、最高得票数は投票配列のうち基
10 準位置に対応する配列要素に集中する。従って雑音等の影響を考慮して
も、本アルゴリズムにより基準位置を正しく特定することが可能である。
これにより特定された基準位置に基づき、部分画像中からメッセージを
適切に抽出することができる。

なお図17(a)の方法では、メッセージが隠べいされた画像データ
15 をさらに変更するため、ランダム雑音に強いデータ・ハイディング手法
でなければ隠べいされた情報の抽出に失敗する可能性がある。一方同図
(b)の方法では、隠べいされたメッセージは抽出処理の時まで一切変
更されないで、同図(a)の方法よりも雑音に強い。従って、用いる
データ・ハイディング手法のパリエーションは増える。但し、本発明の
20 基準位置に関する位置情報の一部が壊されてしまう可能性があるので注
意が必要である。

F. 具体的な応用例

上記のアルゴリズムを用いたデータ・ハイディング方法及びデータ抽
25 出方法は具体的には、以下のようなシステムにおいて用いることができ
る。

(テレビの映像CMの出現カウント)

CMの注文者にとっては、コマーシャルが注文した回数だけきちんと放送されているかどうかということは重要な問題である。本アルゴリズムを用いて、図18に示すようなシステムを構築すればCMの放送回数を自動的にカウントすることができる。放送局側は、記憶装置、符号化装置、及び放送装置を有している。記憶装置にはコマーシャル画像が記憶されていて、符号化装置はコマーシャル画像の放送回数をカウントするための情報をコマーシャル画像に隠べいためのものである。そして、この情報が符号化装置により隠べいされたコマーシャル画像は放送装置によって放送される。このようなシステムで、上述のデータ・ハイディング方法を用いてコマーシャル画像を符号化する。符号化はカウント情報が有するデータに基づいて行われ、コマーシャル画像中に分散してカウント情報が隠べいされる。また、受信側は、受信装置、復号化装置、及びカウンタを有している。受信装置は上記のカウンタ情報が既に隠べいされているコマーシャル画像を受信する。復号化装置はこのコマーシャル画像からカウンタ情報を抽出する。そして抽出されたカウンタ情報に基づいて、カウンタはコマーシャル画像の放送回数をカウントする。このような受信システムでは、上述のデータ抽出方法を用いてカウンタ情報が抽出される。復号化は、カウンタ情報が有するデータに基づいて、カウンタ情報が分散して存在しているコマーシャル画像上の位置を特定して抽出される。

放送局はCM画像中に、ハイディング・アルゴリズムに基づいて受信側で放送回数をカウントできるようなカウンタ情報をコマーシャル画像に隠べいした上で放送する。従って、受信側ではこのカウンタ情報を抽出することで放送回数をカウントすることができる。

(ファイヤー・ウォールでの検閲)

ファイヤー・ウォール(Firewall)などのトポロジーに位置するプロキシ（代理）には壁の内側と外側のH T T P 通信すべてが流れている。これを利用すれば、そのプロキシ上で画像や音声データを検閲することができる。ウォーター・マークなどが隠ぺいされているメディア・データを検出したらログに残す。このようにすれば不正に流通しているデータを把握することができる。図 1 9 は、このようなシステムのブロック図である。サーバー側はメディア・データが記憶されている記憶手段、及びメッセージ・データをメディア・データに隠ぺいする符号化装置を有している。サーバーは、記憶手段から読み出されたメディア・データ中に、メッセージ・データを隠ぺいするように符号化装置を制御し、この出力データをインターネットに送信する。ここで、上述のようなハイディング方法を用いて、メッセージ・データの内容に基づいてメッセージ・データをメディア・データ中に分散して隠ぺいしていく。一方の受信側は、送信側でハイディング処理されたメディア・データをインターネットから受信するプロキシと、この受信データからメッセージ・データを抽出する復号化装置とを有している。この抽出は、上述のデータ抽出方法を用いて、メッセージ・データの内容に基づいて分散配置されているメッセージ・データの位置を特定した上で行われる。

（旅行代理店サーバでの利用）

旅行代理店の運営するWWWサーバに展示して有る観光地の写真に、その観光地の説明文書や地図、あるいはURLなどのポインタ情報といった付加情報を隠ぺいしておく。WWWブラウザを使ってその写真をネットワーク・コピーしておけば、後に地図等をその写真から取り出して説明文や行き方などを確認することができる。図 2 0 に示すように、クライアントとWWWサーバーとの接続が切断された後であっても、付加情報を抽出することができる。付加情報が写真データなどと別ファイル

になっているような場合と比べて、ハイディングを用いれば写真データと付加情報の密な関係を維持し続けられるので、データの整理が容易である。

(フィンガー・プリンティング及びウォーター・マーキング)

5 フィンガー・プリンティングとは、メディア・データを第三者に発行する際に、発行者が発行先である第三者を特定できるようなマークを予めメディア・データ中に隠ぺいしておくことをいう。このようにしておけば、違法コピーなどの不正な行為が行われれば場合、そのコピーのソースを特定することができる。従って、この第三者が不正に流通している
10 場合には、違法コピー分の料金を請求することができる。

これに対して、ウォーター・マーキングとは、メディア・データを第三者に発行する際に、発行者が発行者自身を特定できるようなマークを予め隠ぺいしておくことをいう。これによって、流通過程で改変されていないことを保証、すなわち、このデータが正規の発行者からのもので
15 あり、かつ途中で改変されていない、ということが保証される。

このようなマークを隠ぺいするために、図21のようなシステムを構築すればよい。第三者への発行の際にはマークを隠ぺいして発行する。検出の場合には、第三者から得られたデータからマークを抽出する。

上記のシステムの他にも、本発明は、ケーブル通信、衛星通信を用いたシステムや、DVD-ROM等の記録媒体を用いたシステム等に広く
20 利用できる。特にDVD-ROM (DVD-RAM) を用いてメディア・データを配布しようとする場合、当該メディア・データ中にコピー許可条件、すなわちコピーを禁止するのか認めるのかという情報を隠蔽した上で配布する。そして、エンド・ユーザがメディア・データを複製する
25 ために用いるDVDプレーヤーには、コピーを制限する機能が設けられている。このようにすることにより、コピー用のプレーヤーが隠蔽され

たコピー許可条件を媒体から抽出・認識し、それがコピー禁止を意味しているならば、コピーを禁止するように動作する。

G. データ抽出システム及びそれを実現する半導体集積回路

5 上述したデータ抽出方法は、具体的には、以下のような構成を有するシステムで実現することができる。また、そのシステムが有する機能の大半はワンチップ化して半導体集積回路とすることができる。なお、これらのシステム及び半導体集積回路の特徴は、重複説明を避けるために詳細な説明は省略するが、データ抽出方法にて説明した事項及びその拡張・変形がそのまま当てはまる。当業者であれば、上記方法の説明で、
10 下記の事項の詳細は理解できよう。

メッセージ・データをメディア・データ中から抽出するシステムは、具体的には、図 22 に示すように、変換手段、特定手段、特性値計算手段、記憶手段、及び抽出手段を有している。変換手段は、メッセージ・データが隠ぺいされたアナログ信号としてのメッセージ・データをデジタル信号に変換した上で、デジタル信号を出力する A/D コンバータである。特定手段は、変換手段の出力としてのメディア・データ中において、メッセージ・データが隠ぺいされている一ブロックを特定するためのものである。特性値計算手段は、特定手段により特定された一ブロックの特性値を求めるためのものである。記憶手段中には、特性値の
15 基準を与える基準値とブロックの特性値との大小関係を、抽出すべきデータの内容に対応づけた変換規則が記憶されている。また抽出手段は、変換規則を参照して、一ブロックの特性値に応じて、隠ぺいされているメッセージ・データを抽出する。
20

ここで、基準値は、メディア・データ中に存在しかつ一ブロックとは異なる他のブロックに関する特性値である。また、記憶手段が記憶する変換規則は、一ブロックの特性値が他のブロックの特性値よりも大
25

きい場合、一方のビットを抽出すると規定し、逆の場合には、他方のビットを抽出すると規定している。

また、上記システムをワンチップ化した半導体集積回路は、図 23 に示すように、演算手段と、抽出手段を少なくとも有している。演算手段は、入力信号としてのメディア・データにおいて、メッセージ・データが隠ぺいされているものとして特定された一のブロックに関して特性値を求める手段である。また、抽出手段は、特性値の基準を与える基準値とブロックの特性値との大小関係を、抽出すべきデータの内容に対応づけた変換規則を参照して、一のブロックの特性値に応じて、隠ぺいされているメッセージ・データを抽出する手段である

〔産業上の利用可能性〕

このように、本発明では、画像や音声といったメディア・データにメッセージ・データを分散してハイディングする場合に、メディア・データの内容とメッセージ・データの内容に基づいて、メッセージを隠ぺいする位置を決定しているので、第三者がメッセージを改変することが困難なデータ・ハイディングを行うことが可能となる。

請 求 の 範 囲

1. メディア・データがメディア配列として表現されると共に、メッセージ・データがメッセージ配列として表現されており、前記メディア配列中の特定の配列要素を指定する状態値に基づいて、前記メッセージ配列の配列要素を分散して前記メディア配列に隠ぺいするデータ・ハイディング方法において、
- 5 (a) j ($j \geq 0$) 番目の状態値を決定するステップと、
- 10 (b) 前記 j 番目の状態値と、当該 j 番目の状態値により指定される前記メディア配列の配列要素と、前記メッセージ配列の配列要素とに基づいて、 $(j + 1)$ 番目の状態値を決定するステップと、
- (c) 前記 $(j + 1)$ 番目の状態値が指定する前記メディア配列の配列要素に対して、データを隠ぺいするステップと
- 15 を有することを特徴とするデータ・ハイディング方法。
2. メディア・データがメディア配列として表現されると共に、メッセージ・データがメッセージ配列として表現されており、前記メディア配列中の特定の配列要素を指定する状態値に基づいて、前記メッセージ配列の J 個の配列要素を分散して前記メディア配列に隠ぺいするデータ・
- 20 ハイディング方法において、
- (a) j ($j \geq 0$) 番目の状態値を決定するステップと、
- (b) 前記 j 番目の状態値と、当該 j 番目の状態値により指定される前記メディア配列の配列要素と、前記メッセージ配列の配列要素とに基づいて、 $(j + 1)$ 番目の状態値を決定するステップと、
- 25 (c) 前記 $(j + 1)$ 番目の状態値が指定する前記メディア配列の配列要素に対して、データを隠ぺいするステップと、

(d) 上記ステップ(a)乃至(c)を再帰的に実行することにより、前記メッセージ配列のJ個の配列要素を隠ぺいするステップと

を有することを特徴とするデータ・ハイディング方法。

5 3. 上記ステップ(a)において、 $j = 0$ の場合、最初の状態値は、前記メッセージ配列の配列要素が有するデータに基づいて決定されることを特徴とする請求項1または2に記載のデータ・ハイディング方法。

4. 最初の状態値を決定する初期関数を用意し、

10 上記ステップ(a)において、 $j = 0$ の場合には、前記メッセージ配列のすべての配列要素が有するデータの排他的論理和を前記初期関数の入力として、前記初期関数の出力を前記最初の状態値とすることを特徴とする請求項1または2に記載のデータ・ハイディング方法。

15 5. 上記ステップ(b)において、前記($j + 1$)番目の状態値は、前記j番目の状態値と、当該j番目の状態値により指定される前記メディア配列の配列要素が有するデータと、前記メッセージ配列の配列要素が有するデータとの排他的論理和に基づいて、決定されることを特徴とする請求項1または2に記載のデータ・ハイディング方法。

6. ハイディング用位置変換関数を用意し、

20 上記ステップ(b)において、前記j番目の状態値と、当該j番目の状態値により指定される前記メディア配列の配列要素が有するデータと、前記メッセージ配列の配列要素が有するデータとの排他的論理和を前記位置変換関数の入力とし、前記位置変換関数の出力を前記($j + 1$)番目の状態値とすることを特徴とする請求項1または2に記載のデータ・ハイディング方法。

25 7. 前記ハイディング用位置変換関数は、公開鍵方式における秘密鍵をパラメータとした暗号化関数であることを特徴とする請求項6に記載のデータ・ハイディング方法。

8. 上記ステップ(c)において、前記ハイディング・データは、前記 j 番目の状態値により指定される前記メディア配列の配列要素と前記メッセージ配列の配列要素との排他的論理和であることを特徴とする請求項 1 または 2 に記載のデータ・ハイディング方法。
- 5 9. 上記ステップ(c)において、前記 $(j + 1)$ 番目の状態値が指定する前記メディア配列の配列要素に対応する一のピクセル・ブロックと、他のピクセル・ブロックとでペアを形成し、変換規則に基づいて、ピクセル・ブロックの特性値を操作することにより、ハイディング・データが隠ぺいされることを特徴とする請求項 1 または 2 に記載のデータ・ハイディング方法。
- 10 10. 前記他のピクセル・ブロックは、ペアを構成する前記一のピクセル・ブロックに隣接していることを特徴とする請求項 9 に記載のデータ・ハイディング方法。
- 15 11. 前記変換規則はペアを構成するそれぞれのピクセル・ブロックが有する特性値の大小関係に基づいて、前記特性値の操作の規則を規定していることを特徴とする請求項 9 に記載のデータ・ハイディング方法。
12. 前記特性値は、前記ピクセル・ブロックが有する輝度値であることを特徴とする請求項 11 に記載のデータ・ハイディング方法。
13. 前記特性値は、前記ピクセル・ブロックが有する分散値であることを特徴とする請求項 11 に記載のデータ・ハイディング方法。
- 20 14. (d) 前記ハイディング・データが隠ぺいされた前記メディア配列と最後の状態値とを抽出するステップとをさらに有することを特徴とする請求項 2 に記載のデータ・ハイディング方法。
- 25 15. メッセージ・データがメッセージ配列として表現され、前記メッセージ・データを含んだハイディング・データがハイディング配列とし

て表現され、かつ前記ハイディング・データが分散して隠ぺいされているメディア・データがメディア配列として表現されていて、前記メディア配列中の特定の配列要素を指定する状態値に基づいて、前記メディア配列から前記メッセージ配列を抽出するデータ抽出方法において、

- 5 (a) j ($j \geq 1$) 番目の状態値を決定するステップと、
(b) 前記 j 番目の状態値により指定される前記メディア配列の配列要素から、前記ハイディング配列の配列要素を抽出するステップと、
(c) 前記 j 番目の状態値と、抽出された前記ハイディング配列の配列要素に基づいて、($j - 1$) 番目の状態値を決定するステップと、
10 (d) 前記 ($j - 1$) 番目の状態値が指定する前記メディア配列の配列要素及び抽出された前記ハイディング配列の配列要素に基づいて、前記メッセージ配列の配列要素を抽出するステップと
を有することを特徴とするデータ抽出方法。

- 1 6. メッセージ・データがメッセージ配列として表現され、前記メッセージ・データを含んだハイディング・データがハイディング配列として表現され、かつ前記ハイディング・データが分散して隠ぺいされているメディア・データがメディア配列として表現されていて、前記メディア配列中の特定の配列要素を指定する状態値に基づいて、前記メディア配列から前記メッセージ配列を抽出するデータ抽出方法において、

- 15 (a) j ($j \geq 1$) 番目の状態値を決定するステップと、
(b) 前記 j 番目の状態値により指定される前記メディア配列の配列要素から、前記ハイディング配列の配列要素を抽出するステップと、
(c) 前記 j 番目の状態値と、抽出された前記ハイディング配列の配列要素に基づいて、($j - 1$) 番目の状態値を決定するステップと、
20 (d) 前記 ($j - 1$) 番目の状態値が指定する前記メディア配列の配列要素及び抽出された前記ハイディング配列の配列要素に基づいて、前記メ

ッセージ配列の配列要素を抽出するステップと、

(e) 抽出終了条件を満たすまで、上記ステップ(a)乃至(c)を再帰的に実行するステップと

を有することを特徴とするデータ抽出方法。

5 17. 上記ステップ(a)において、抽出を開始する際に最初に用いる状態値は、抽出に必要な情報として抽出者に予め与えられていることを特徴とする請求項15または16に記載のデータ抽出方法。

10 18. 上記抽出を開始する際に最初に用いる状態値は、前記メッセージ配列を隠ぺいする際に生成された最後の状態値であることを特徴とする請求項17に記載のデータ抽出方法。

15 19. 上記ステップ(c)において、前記(j-1)番目の状態値は、前記j番目の状態値と、当該j番目の状態値により指定される前記メディア配列の配列要素から抽出された前記ハイディング配列の配列要素が有するデータとの排他的論理和に基づいて、決定されることを特徴とする請求項15または16に記載のデータ抽出方法。

20 20. 抽出用位置変換関数を用意し、

 上記ステップ(c)において、前記j番目の状態値と、前記j番目の状態値により指定される前記メディア配列の配列要素から抽出された前記ハイディング配列の配列要素が有するデータとの排他的論理和を前記位置変換関数の入力とし、前記位置変換関数の出力を前記(j-1)番目の状態値とすることを特徴とする請求項15または16に記載のデータ抽出方法。

25 21. 前記抽出用位置変換関数は、公開鍵方式における公開鍵をパラメータとした復号化関数であることを特徴とする請求項20に記載のデータ抽出方法。

 22. 上記ステップ(b)において、前記ハイディング配列の配列要素は、

前記 (j - 1) 番目の状態値により指定される前記メディア配列の配列要素と前記メッセージ配列の配列要素との排他的論理和であることを特徴とする請求項 15 または 16 に記載のデータ抽出方法。

5 23. 上記ステップ (b) において、前記 j 番目の状態値が指定する前記メディア配列の配列要素に対応するピクセル・ブロックと、他のピクセル・ブロックとでペアを形成し、ペアを構成する前記ピクセル・ブロックの特性値の関係から、抽出規則に基づいて、隠ぺいされたデータを抽出することを特徴とする請求項 15 または 16 に記載のデータ・ハイディング方法。

10 24. 前記他のピクセル・ブロックは、ペアを構成する前記一のピクセル・ブロックに隣接していることを特徴とする請求項 23 に記載のデータ抽出方法。

15 25. 前記抽出規則は、ペアを構成するそれぞれの前記ピクセル・ブロックが有する特性値の大小関係に基づいており、かつハイディング時における前記特性値の操作を規定した変換規則に対応していることを特徴とする請求項 23 に記載のデータ抽出方法。

26. 前記特性値は、前記ピクセル・ブロックが有する輝度値であることを特徴とする請求項 25 に記載のデータ抽出方法。

20 27. 前記特性値は、前記ピクセル・ブロックが有する分散値であることを特徴とする請求項 25 に記載のデータ抽出方法。

28. データをハイディングする際に用いられる、前記メッセージ配列の配列要素が有するデータに基づいて、最初の状態値を決定する初期関数を用意し、

25 (f) 上記ステップ (d) において、前記メッセージ配列の要素が抽出されるごとに、すでに抽出されたすべての前記メッセージ配列の配列要素が有するデータを前記初期関数の入力とし、前記初期関数の出力が前記 (

j - 1) 番目の状態値と一致することを前記抽出終了条件として判断するステップと

をさらに有することを特徴とする請求項 16 に記載のデータ抽出方法。

29. すでに抽出されたすべての前記メッセージ配列の配列要素が有するデータの排他的論理和を、前記初期関数の入力とすることを特徴とする請求項 28 に記載のデータ抽出方法。

30. ステップ(f)において、前記初期関数の出力が前記(j - 1)番目の状態値と一致する場合に抽出終了と認めることを特徴とする請求項 27 に記載のデータ抽出方法。

31. コマーシャル画像が記憶されている記憶装置と、

前記コマーシャル画像の放送回数をカウントするための情報を、前記コマーシャル画像に隠ぺいする符号化装置と、

前記情報が隠ぺいされた前記コマーシャル画像を放送する放送装置とを有し、

カウントするための前記情報が有するデータに基づいて、前記情報は、前記コマーシャル画像中に分散して隠ぺいされていることを特徴とする放送システム。

32. 前記情報を前記コマーシャル画像に隠ぺいする方法は、請求項 1 乃至 14 のいずれかに記載されたデータ・ハイディング方法であることを特徴とする請求項 31 に記載の放送システム。

33. コマーシャル画像中に前記コマーシャル画像の放送回数をカウントするための情報が隠ぺいされていて、係る前記コマーシャル画像を受信する受信装置と、

前記コマーシャル画像から前記情報を抽出する復号化装置と、

抽出された前記情報に基づいて、前記コマーシャル画像の放送回数をカウントするカウンタとを有し、

カウントするための前記情報が有するデータに基づいて、分散して隠
べいされている前記情報の前記コマーシャル画像中の位置を特定して抽
出することを特徴とする受信システム。

34. 前記情報を前記コマーシャル画像から抽出する方法は、請求項 1
5 乃至 30 のいずれかに記載されたデータ抽出方法であることを特徴
とする請求項 33 に記載の受信システム。

35. メディア・データが記憶された記憶手段と、

メッセージ・データを前記メディア・データに隠べいする符号化装置
と、

10 前記記憶手段から読み出された前記メディア・データ中に、前記メッ
セージ・データを隠べいするように符号化装置を制御し、前記符号化装
置の出力データをネットワークに送信するサーバーとを有し、

前記メッセージ・データの内容に基づいて、前記メッセージ・データ
は、前記メディア・データ中に分散して隠べいされていることを特徴と
15 するネットワークにデータを送信するシステム。

36. 前記隠べいする方法は、請求項 1 乃至 14 のいずれかに記載さ
れたデータ・ハイディング方法であることを特徴とする請求項 35 に記
載のネットワークにデータを送信するシステム。

37. メッセージ・データが隠べいされているメディア・データをネット
20 ワークから受信する受信装置と、

前記メディア・データから前記メッセージ・データを抽出する復号化
装置とを有し、

前記メッセージ・データの内容に基づいて、分散して隠べいされてい
る前記メッセージ・データの前記メディア・データ中の位置を特定して
25 抽出することを特徴とするネットワークからデータを受信するシステム。

38. 前記抽出する方法は、請求項15乃至30のいずれかに記載されたデータ抽出方法であることを特徴とする請求項37に記載のネットワークからデータを受信するシステム。

5 39. 第1のデータが第1の配列として表現されると共に、第2のデータが第2の配列として表現されており、前記第1の配列中の特定の配列要素を指定する状態値に基づいて、前記第2の配列要素を分散して前記第1の配列に隠ぺいするデータ・ハイディング方法において、

(a) j ($j \geq 0$) 番目の状態値を決定するステップと、
(b) 前記 j 番目の状態値と、当該 j 番目の状態値により指定される前記第1の配列の配列要素と、前記第2の配列の配列要素とに基づいて、
10 ($j + 1$) 番目の状態値を決定するステップと、

(c) 前記 ($j + 1$) 番目の状態値が指定する前記第1の配列の配列要素に対して、データを隠ぺいするステップと

を有することを特徴とするデータ・ハイディング方法。

15 40. 第2のデータが第2の配列として表現され、前記第2のデータを含んだ第3のデータが第3の配列として表現され、かつ前記第3のデータが分散して隠ぺいされている第1のデータが第1の配列として表現されていて、前記第1の配列中の特定の配列要素を指定する状態値に基づいて、前記第1の配列から前記第2の配列を抽出するデータ抽出方法において、

20 (a) j ($j \geq 1$) 番目の状態値を決定するステップと、
(b) 前記 j 番目の状態値により指定される前記第1の配列の配列要素から、前記第3の配列の配列要素を抽出するステップと、

(c) 前記 j 番目の状態値と、抽出された前記第3の配列の配列要素に基づいて、($j - 1$) 番目の状態値を決定するステップと、

25 (d) 前記 ($j - 1$) 番目の状態値が指定する前記第1の配列の配列要素

及び抽出された前記第3の配列の配列要素に基づいて、前記第2の配列の配列要素を抽出するステップと

を有することを特徴とするデータ抽出方法。

5 41. メディア・データにデータを隠ぺいするデータ・ハイディング方法において、

前記メッセージ・データ中に、前記メッセージ・データ及び前記メディア・データの基準位置に関する情報を隠ぺいし、

10 前記基準位置に関する情報は、前記メッセージ・データ中に隠ぺいされていて、かつ、前記メッセージ・データの一部分が部分メッセージ・データとして切り取られた場合においても、前記部分メッセージ・データから、本来のメッセージ・データの前記基準位置または前記基準位置に基づく相対的な位置を検出できる情報である

ことを特徴とするデータ・ハイディング方法。

15 42. 前記基準位置に関する情報は、前記基準位置を中心とした描かれた同心円弧であることを特徴とする請求項41に記載のデータ・ハイディング方法。

43. メディア・データ中にメッセージ・データを隠ぺいするデータ・ハイディング方法において、

20 (a) メッセージ・データを隠ぺいすべき一のブロックをメディア・データ中において特定するステップと、

(b) 特定された前記一のブロックの特性値を求めるステップと、

(c) 隠ぺいすべきデータの内容を、特性値の基準を与える基準値と前記ブロックの特性値との大小関係に対応づけた変換規則を参照して、前記一のブロックの特性値を操作することによりメッセージ・データを隠ぺいするステップと

25 を有することを特徴とするデータ・ハイディング方法。

4 4 . 前記基準値は、メディア・データ中に存在する他のブロックの特性値により与えられることを特徴とする請求項 4 3 に記載のデータ・ハイディング方法。

5 4 5 . メディア・データ中にメッセージ・データを隠ぺいするデータ・ハイディング方法において、

(a) 一のブロック及び他のブロックとで構成されるペアを、メディア・データ中において特定するステップと、

(b) 前記ペアを構成するそれぞれの前記ブロックの特性値を求めるステップと、

10 (c) 求められた前記特性値の大小関係を比較して、変換規則に基づいて、前記ペアを構成するそれぞれの前記ブロックの特性値を操作することにより、メッセージ・データ中の一部のデータを隠ぺいするステップと、

(d) 全てのメッセージ・データを隠ぺいするために、上記のステップ(a)乃至(c)を繰り返し実行するステップと

15 を有することを特徴とするデータ・ハイディング方法。

4 6 . メディア・データ中にメッセージ・データを隠ぺいするデータ・ハイディング方法において、

(a) 一のブロック及び他のブロックとでペアを構成されるペアを、メディア・データ中において特定するステップと、

20 (b) 前記ペアを構成するそれぞれの前記ブロックの特性値を求めるステップと、

(c) 求められた前記特性値の大小関係を規定した変換規則に基づいて、前記ペアを構成するそれぞれの前記ブロックの特性値を入れ替えることにより、メッセージ・データを隠ぺいするステップと

25 を有することを特徴とするデータ・ハイディング方法。

4 7 . 前記他のブロックは、ペアを構成する前記一のブロックに隣接し

ていることを特徴とする請求項 4 4、4 5 または 4 6 に記載のデータ・ハイディング方法。

4 8. 前記変換規則は、前記一のブロックの特性値が前記他のブロックの特性値よりも大きい場合、一方のビットが隠べいされていると規定し、
5 逆の場合には、他方のビットが隠べいされていると規定することを特徴とする請求項 4 4、4 5 または 4 6 に記載のデータ・ハイディング方法。

4 9. 前記一のブロックの特性値と前記他のブロックの特性値との差が第 1 の閾値より大きい場合には、上記ステップ(c)の実行を禁止するステップとをさらに有し、これによりメディア・データの品質の劣化を抑制することを特徴とする請求項 4 4、4 5 または 4 6 に記載のデータ・ハイディング方法。
10

5 0. 前記一のブロックの特性値と前記他のブロックの特性値との差が第 2 の閾値より小さい場合には、上記ステップ(c)の実行を禁止するステップとをさらに有し、これによりメッセージ・データの抽出精度の低下を抑制することを特徴とする請求項 4 4、4 5 または 4 6 に記載のデータ・ハイディング方法。
15

5 1. 前記ブロックはピクセル・ブロックであり、前記特性値は前記ピクセル・ブロックの輝度値であることを特徴とする請求項 4 4、4 5 または 4 6 に記載のデータ・ハイディング方法。
20

5 2. 前記ブロックはピクセル・ブロックであり、前記特性値は前記ピクセル・ブロックの分散値であることを特徴とする請求項 4 3、4 5 または 4 6 に記載のデータ・ハイディング方法。

5 3. メッセージ・データが隠べいされたメディア・データ中からメッセージ・データを抽出するデータ抽出方法において、
25 (a) メッセージ・データが隠べいされている一のブロックをメディア・

データ中において特定するステップと、

(b) 特定された前記一のブロックの特性値を求めるステップと、

(c) 特性値の基準を与える基準値と前記ブロックの特性値との大小関係を、抽出すべきデータの内容に対応づけた変換規則を参照して、前記一のブロックの特性値に応じて、隠ぺいされているメッセージ・データを抽出するステップと

を有することを特徴とするデータ抽出方法。

5 4. 前記基準値は、メディア・データ中に存在し、かつ前記一のブロックとは異なる他のブロックに関する特性値であることを特徴とする請求項 5 3 に記載のデータ抽出方法。

5 5. メッセージ・データが隠ぺいされたメディア・データ中からメッセージ・データを抽出するデータ抽出方法において、

(a) メッセージ・データが隠ぺいされている、一のブロック及び他のブロックのペアを、メディア・データ中において特定するステップと、

(b) 前記ペアを構成するそれぞれの前記ブロックの特性値を求めるステップと、

(c) 前記ペアを構成するそれぞれの前記ブロックの特性値の大小関係を、抽出すべきデータの内容に対応づけた変換規則を参照して、それぞれの前記ブロックの特性値に応じて、隠ぺいされているメッセージ・データを抽出するステップと

を有することを特徴とするデータ抽出方法。

5 6. 前記他のブロックは、ペアを構成する前記一のブロックに隣接していることを特徴とする請求項 5 4 または 5 5 に記載のデータ抽出方法。

5 7. 前記変換規則は、前記一のブロックの特性値が前記他のブロックの特性値よりも大きい場合、一方のビットを抽出すると規定し、逆の場

合には、他方のビットを抽出すると規定することを特徴とする請求項 5 4 または 5 5 に記載のデータ抽出方法。

5 5 8. 前記変換規則は、ペアを構成する前記一のブロック及び前記他のブロックの特性値の差が所定の閾値より小さい場合には、当該ペアにはメディア・データが隠べいされていないと判断することを特徴とする請求項 5 4 または 5 5 に記載のデータ抽出方法。

5 9. 前記ブロックはピクセル・ブロックであり、前記特性値は前記ピクセル・ブロックの輝度値であることを特徴とする請求項 5 3 または 5 5 に記載のデータ抽出方法。

10 6 0. 前記ブロックはピクセル・ブロックであり、前記特性値は前記ピクセル・ブロックの分散値であることを特徴とする請求項 5 3 または 5 5 に記載のデータ抽出方法。

6 1 メッセージ・データが隠べいされたメディア・データ中から隠べいされたメッセージ・データを抽出するデータ抽出システムにおいて、

15 メッセージ・データが隠べいされた、アナログ信号としてのメッセージ・データをデジタル信号に変換して、出力する変換手段と、

前記変換手段の出力としてのメディア・データ中において、メッセージ・データが隠べいされている一のブロックを特定する特定手段と、

20 前記特定手段により特定された前記一のブロックの特性値を求める特性値計算手段と、

特性値の基準を与える基準値と前記ブロックの特性値との大小関係を、抽出すべきデータの内容に対応づけた変換規則を記憶する記憶手段と、

前記変換規則を参照して、前記一のブロックの特性値に応じて、隠べいされているメッセージ・データを抽出する抽出手段と

25 を有することを特徴とするデータ抽出システム。

6 2. 前記基準値は、メディア・データ中に存在し、かつ前記一のプロ

ックとは異なる他のブロックに関する特性値であることを特徴とする請求項 6 1 に記載のデータ抽出システム。

5 6 3. 前記変換規則は、前記一のブロックの特性値が前記他のブロックの特性値よりも大きい場合、一方のビットを抽出すると規定し、逆の場合には、他方のビットを抽出すると規定することを特徴とする請求項 6 1 に記載のデータ抽出システム。

6 4. メッセージ・データが隠べいされたメディア・データ中からメッセージ・データを抽出する半導体集積回路において、

10 入力信号としてのメディア・データにおいて、メッセージ・データが隠べいされているものとして特定された一のブロックに関して特性値を求める手段と、

15 特性値の基準を与える基準値とブロックの特性値との大小関係を、抽出すべきデータの内容に対応づけた変換規則を参照して、前記一のブロックの特性値に応じて、隠べいされているメッセージ・データを抽出する抽出手段と

を有することを特徴とする半導体集積回路。

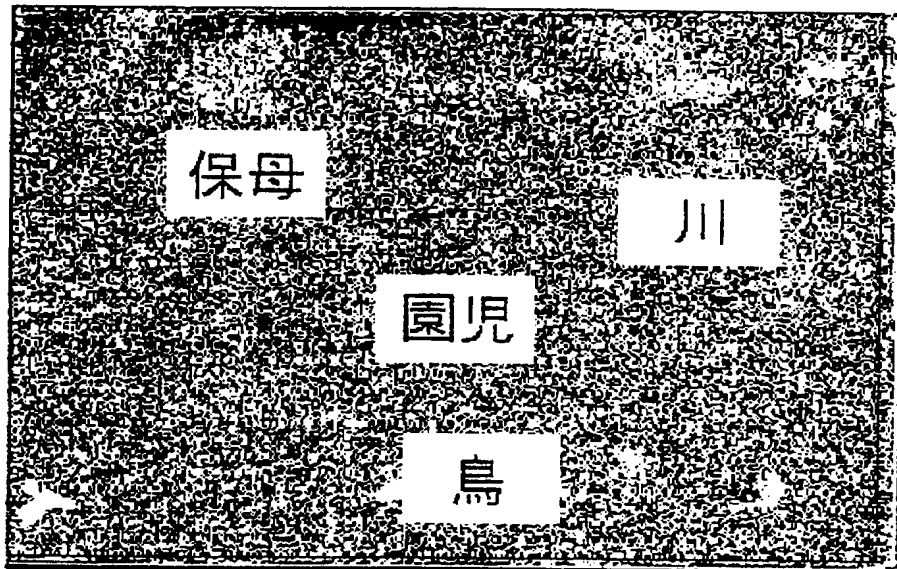
6 5. 前記基準値は、メディア・データ中に存在し、かつ前記一のブロックとは異なる他のブロックに関する特性値であることを特徴とする請求項 6 4 に記載の半導体集積回路。

20 6 6. 前記変換規則は、前記一のブロックの特性値が前記他のブロックの特性値よりも大きい場合、一方のビットを抽出すると規定し、逆の場合には、他方のビットを抽出すると規定することを特徴とする請求項 6 5 に記載の半導体集積回路。

1/17



(a)



(b)

FIG. 1

2 / 17

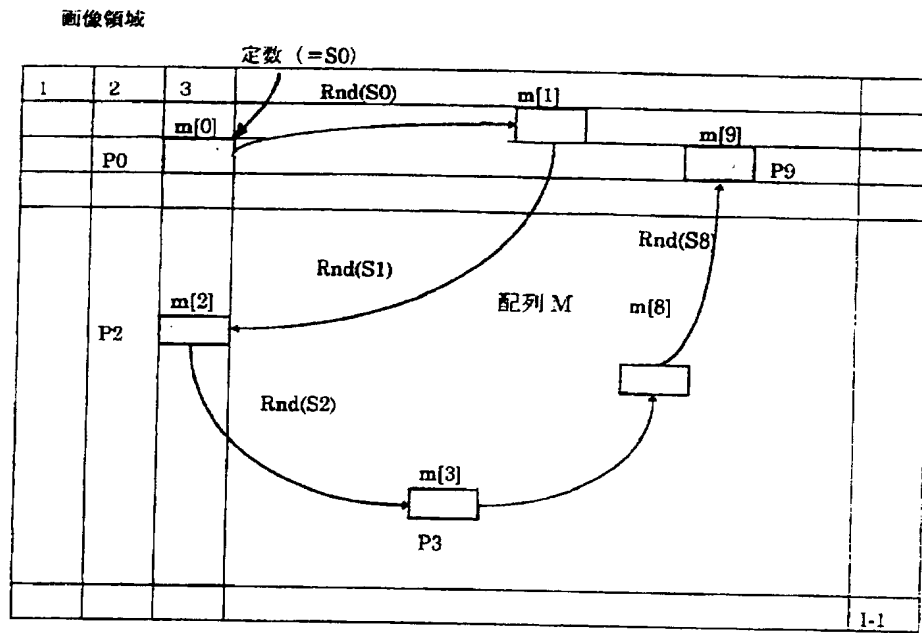


FIG. 2

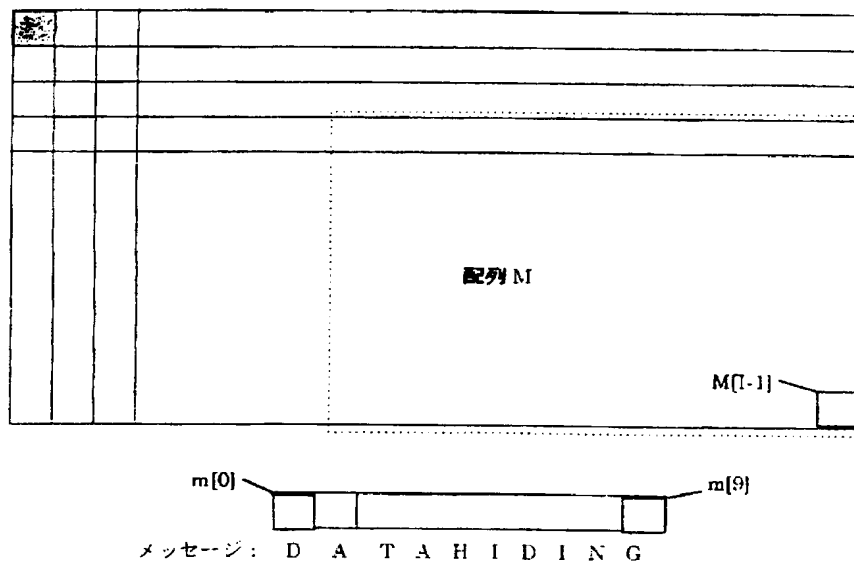


FIG. 3

3 / 17

S0: m 全体により決定(ステップ100)

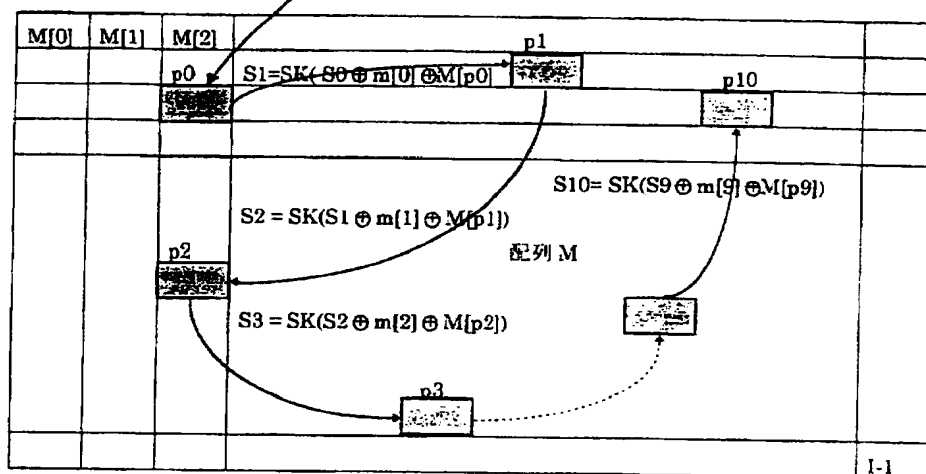


FIG. 4

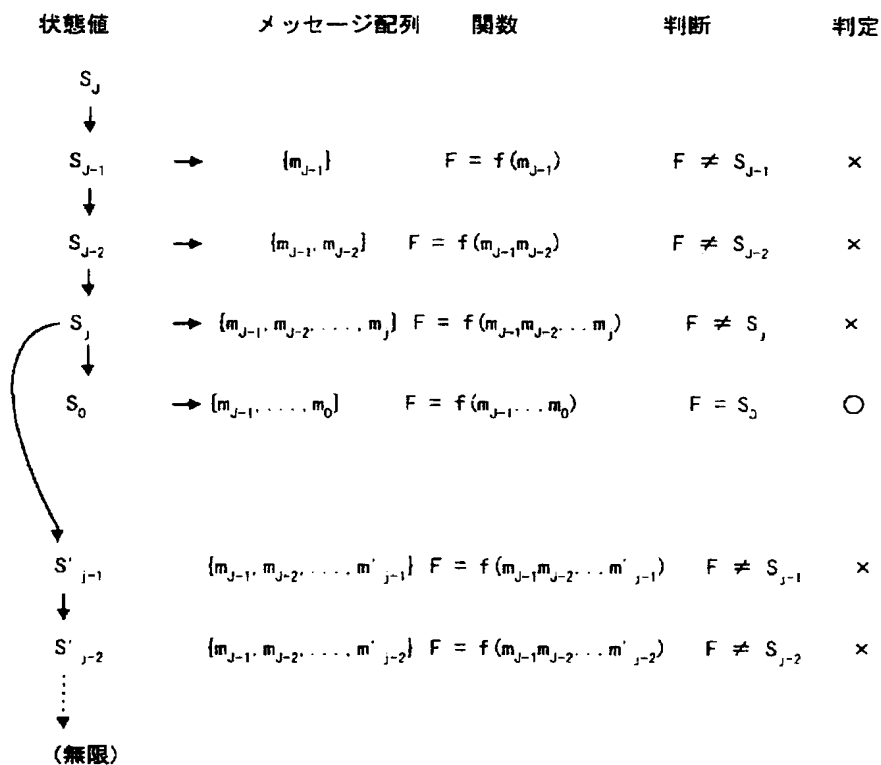


FIG. 10

4 / 17

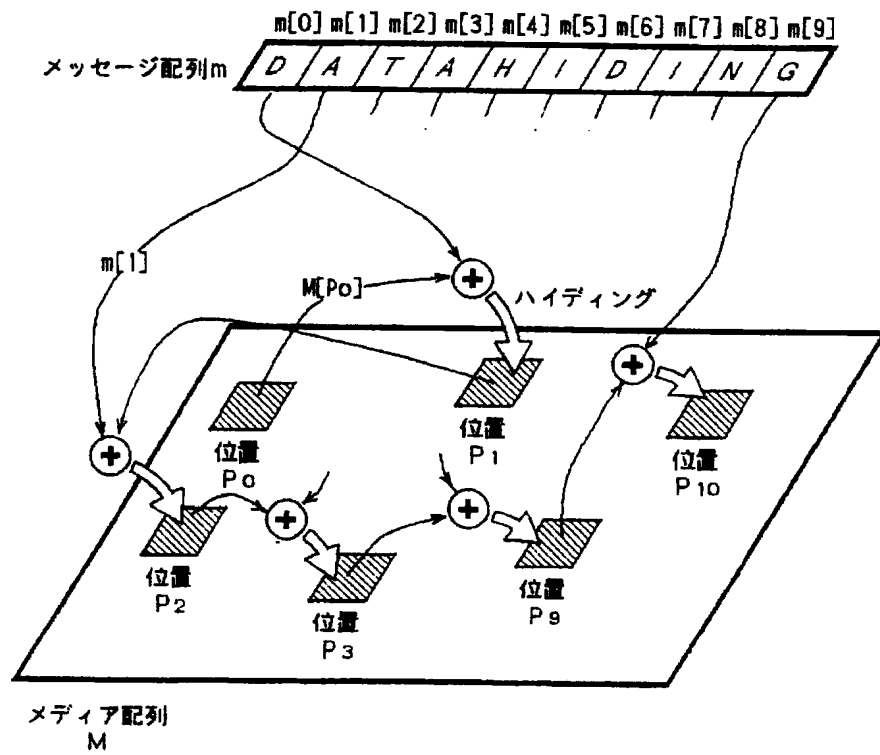


FIG. 5

5 / 1 7

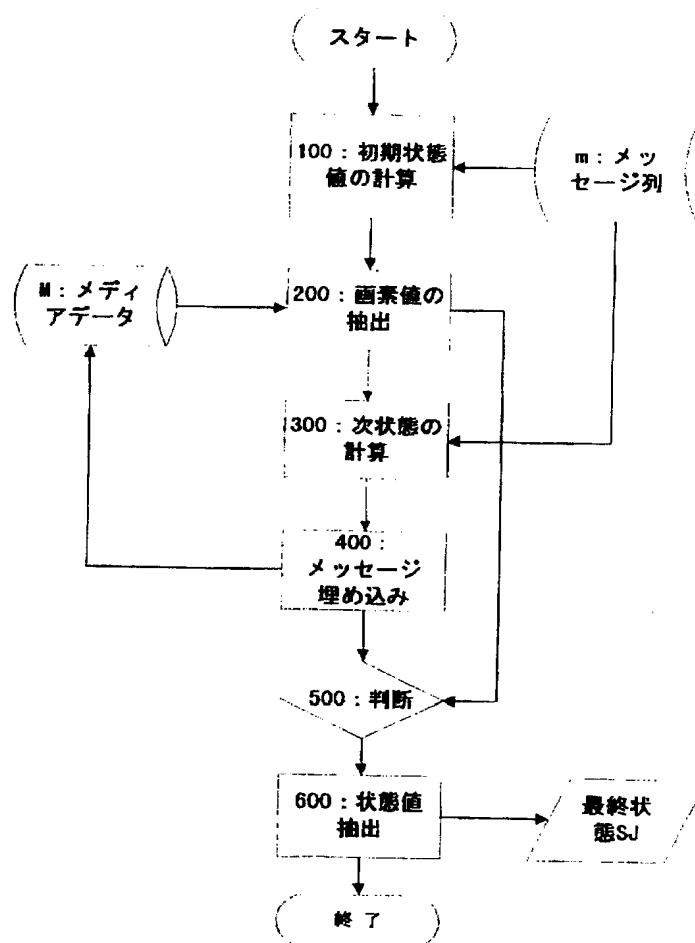
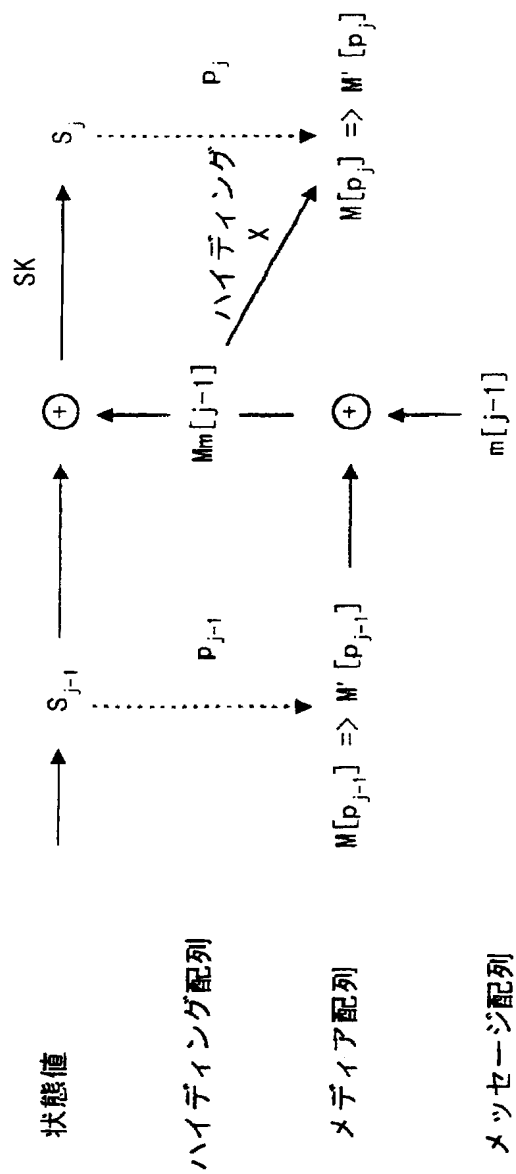


FIG. 6



⊕ : 排他論理和

$2 \leq j \leq J$

FIG. 7

7/17

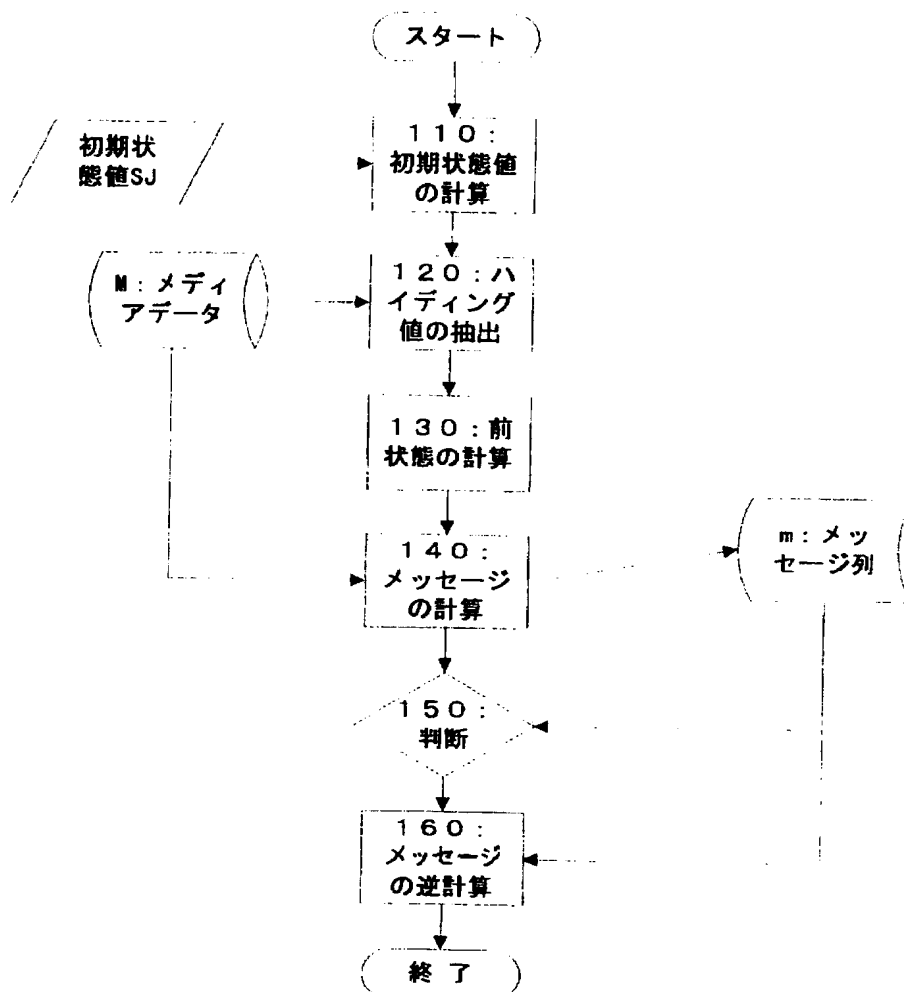
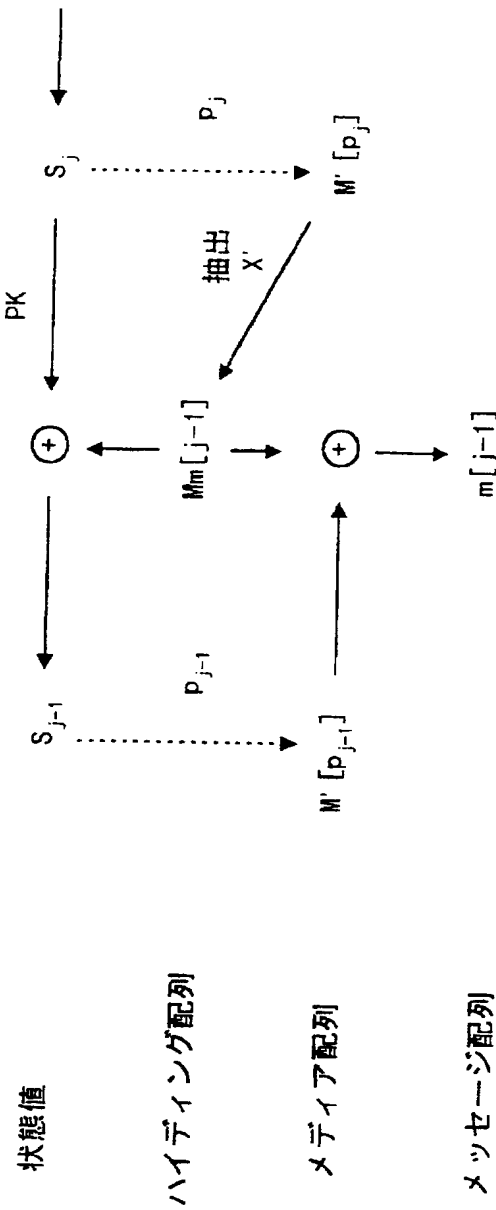


FIG. 8



\oplus : 排他論理和

$1 \leq j \leq J$

FIG. 9

9/17

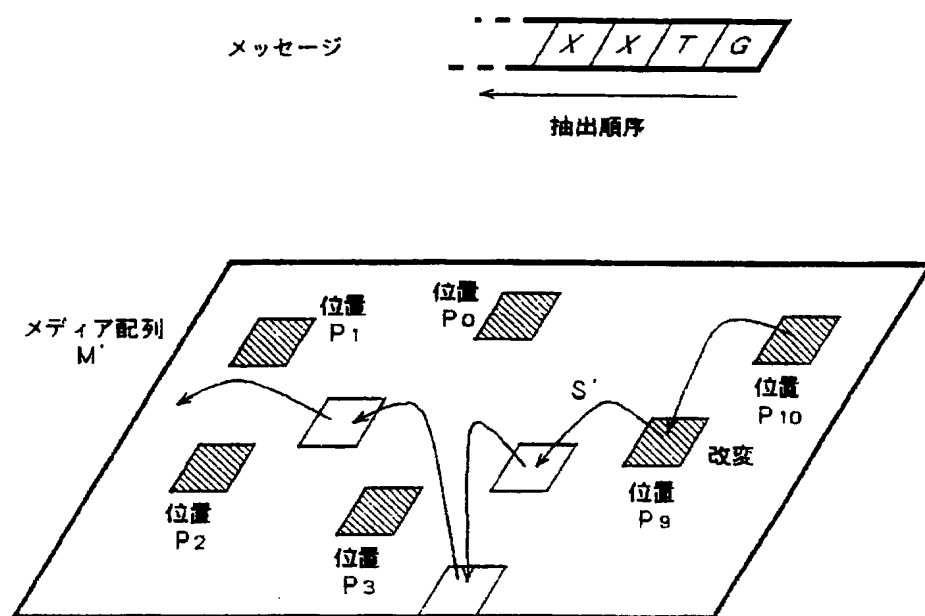
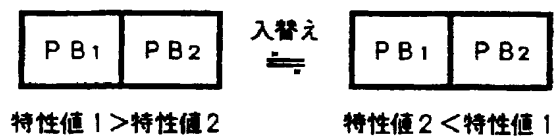
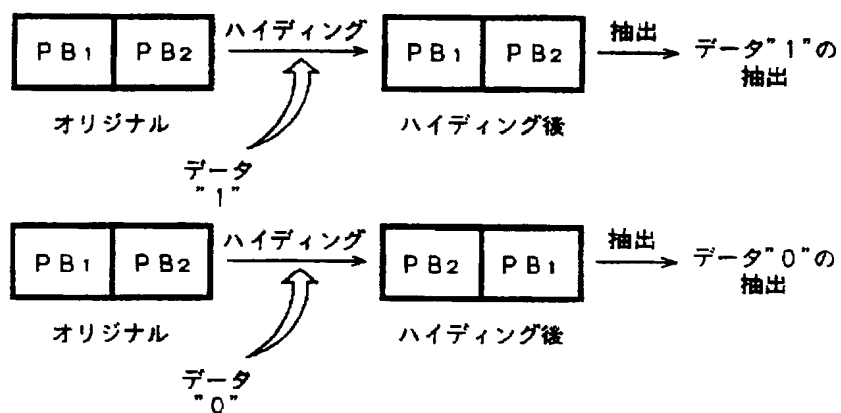


FIG. 11

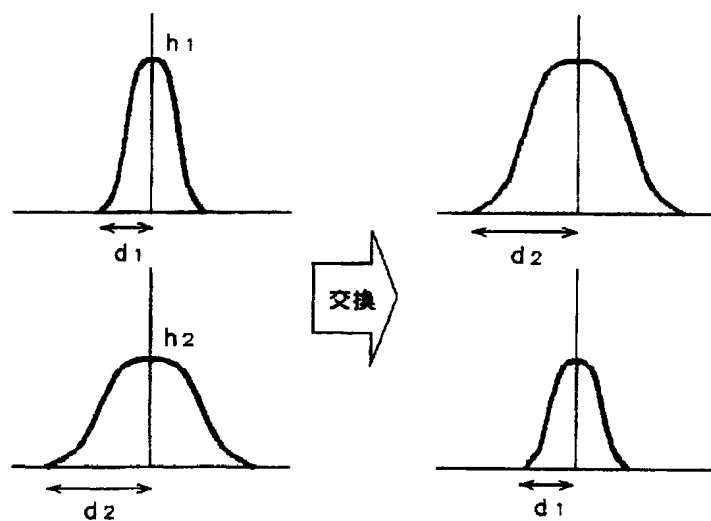
10/17



(a)



(b)



(c)

FIG. 12

二値化された情報

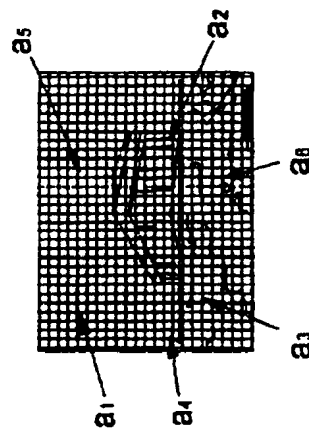
$a = \{011010\}$

画素ブロックの定義

$\boxed{S|L} \rightarrow 0$

$\boxed{L|S} \rightarrow 1$

選択された画素ブロック



画素ブロックの入れ替え処理

data(a)	original		encoded				
$a_1 = \{0\}$	<table><tr><td>122</td><td>135</td></tr></table>	122	135	→	<table><tr><td>122</td><td>135</td></tr></table>	122	135
122	135						
122	135						
$a_2 = \{1\}$	<table><tr><td>101</td><td>125</td></tr></table>	101	125	swap	<table><tr><td>125</td><td>101</td></tr></table>	125	101
101	125						
125	101						
$a_3 = \{1\}$	<table><tr><td>91</td><td>88</td></tr></table>	91	88	→	<table><tr><td>91</td><td>88</td></tr></table>	91	88
91	88						
91	88						
$a_4 = \{0\}$	<table><tr><td>35</td><td>58</td></tr></table>	35	58	→	<table><tr><td>35</td><td>56</td></tr></table>	35	56
35	58						
35	56						
$a_5 = \{1\}$	<table><tr><td>147</td><td>180</td></tr></table>	147	180	swap	<table><tr><td>180</td><td>147</td></tr></table>	180	147
147	180						
180	147						
$a_6 = \{0\}$	<table><tr><td>45</td><td>73</td></tr></table>	45	73	swap	<table><tr><td>73</td><td>45</td></tr></table>	73	45
45	73						
73	45						

FIG. 13

12/17

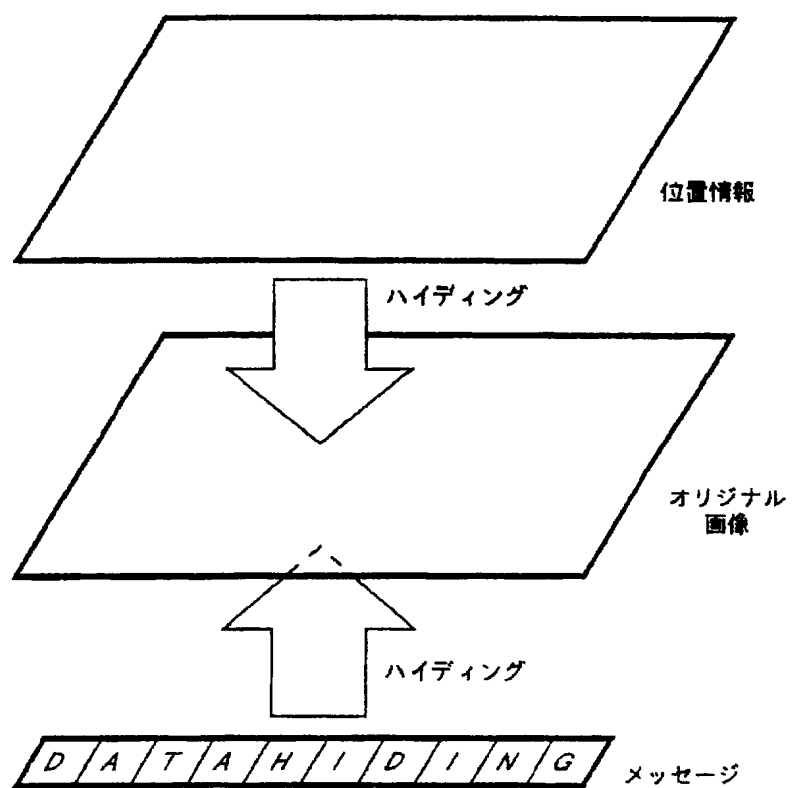


FIG. 14

13/17

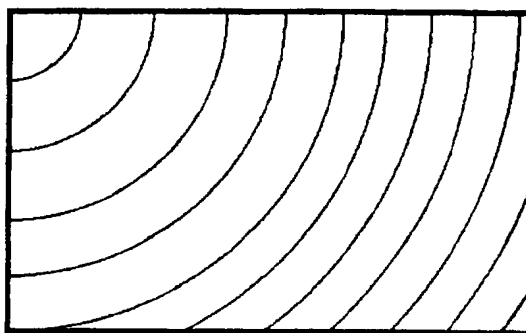


FIG. 15

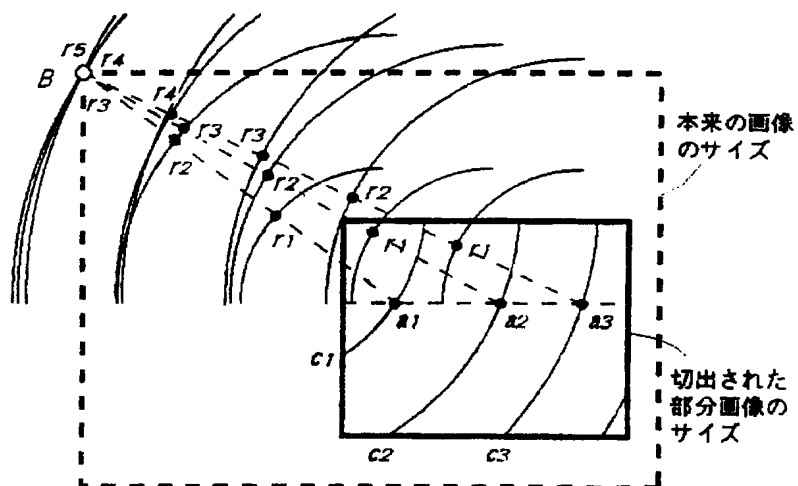


FIG. 16

14/17

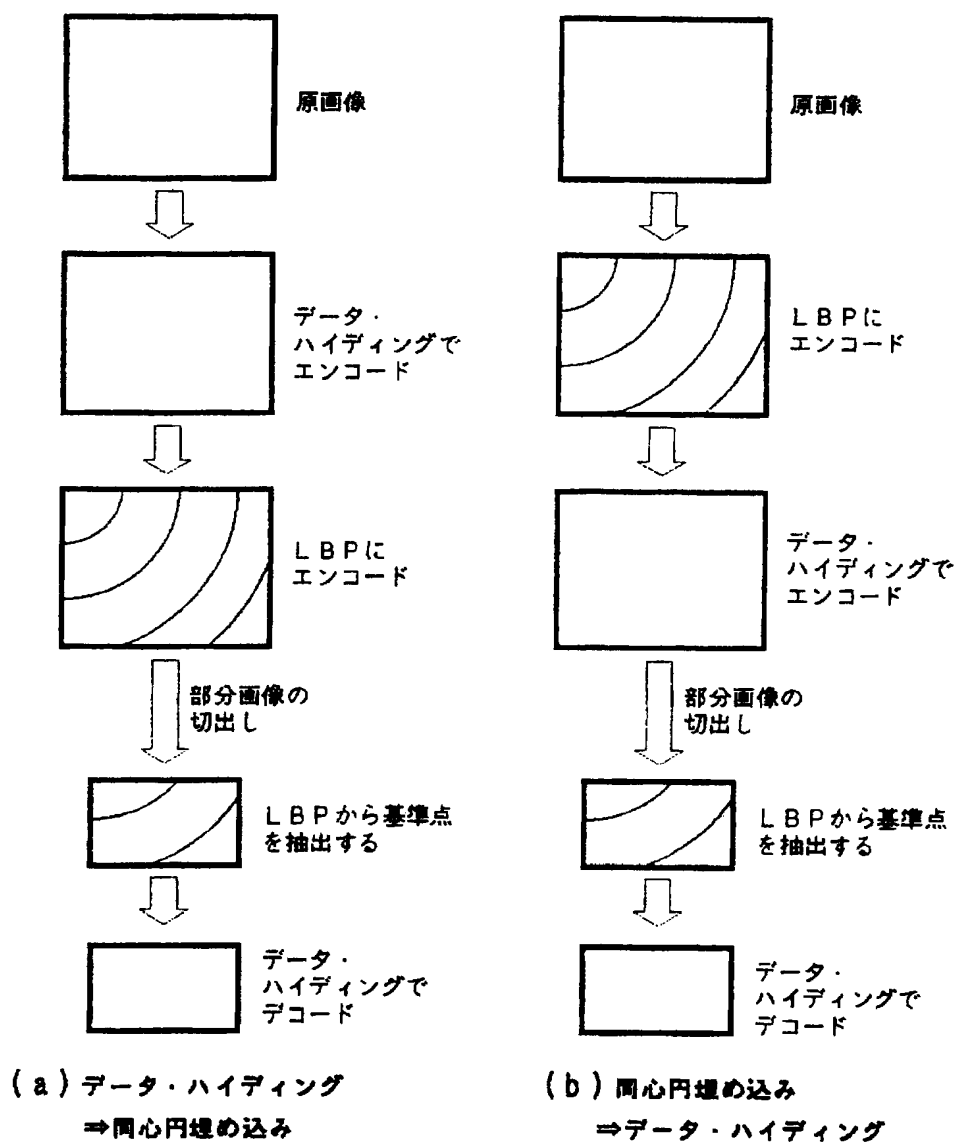


FIG. 17

15/17

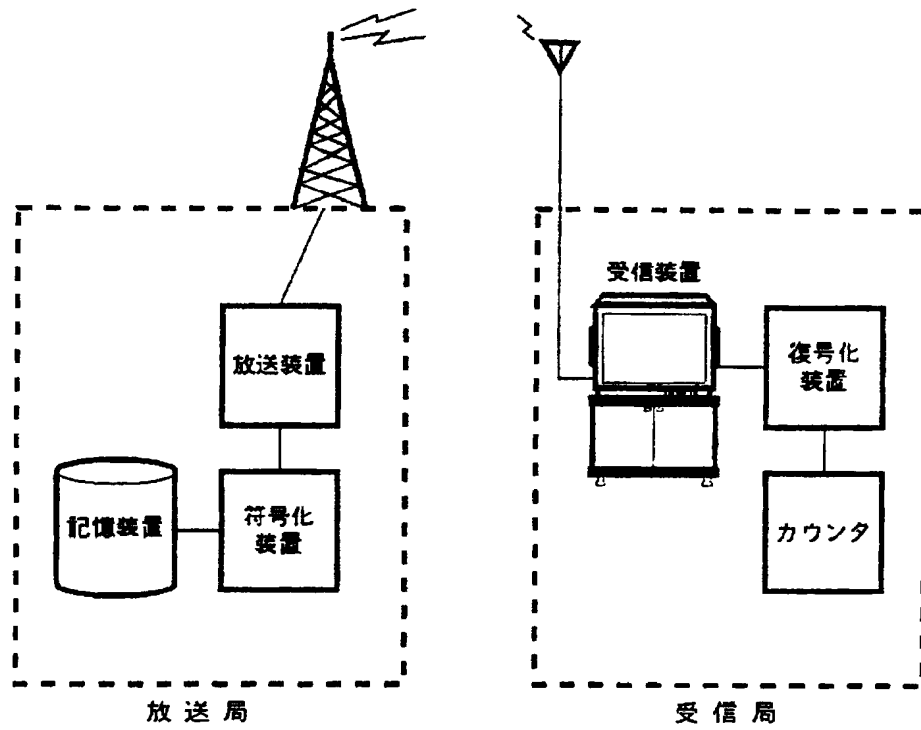


FIG. 18

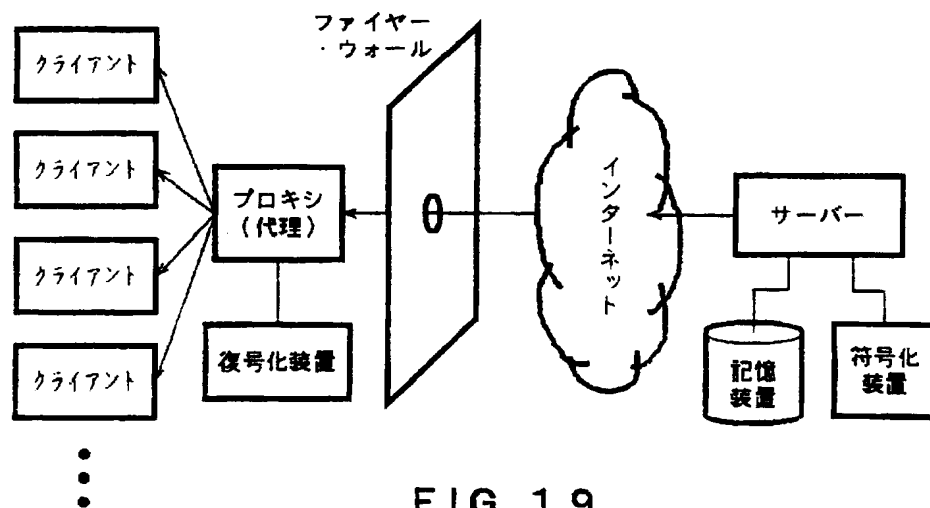


FIG. 19

16/17

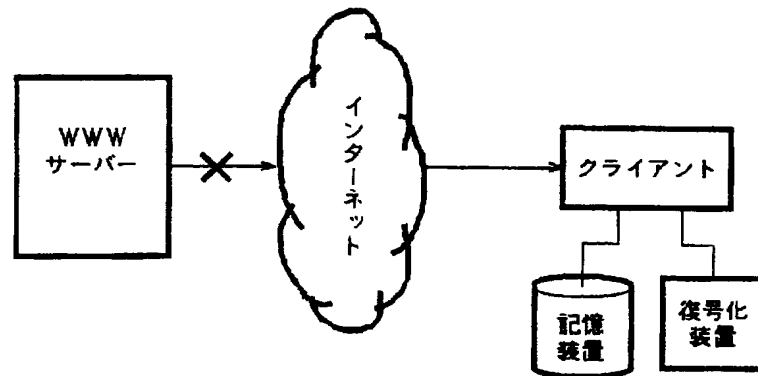


FIG. 20

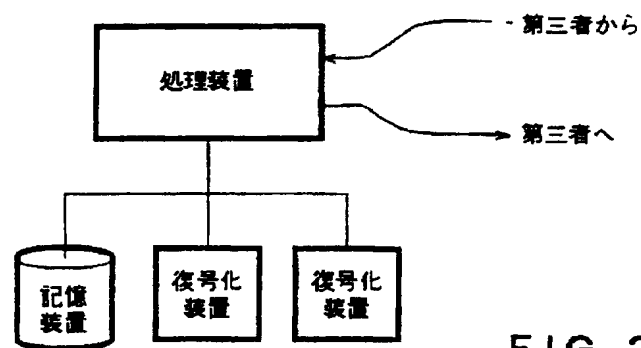


FIG. 21

17/17

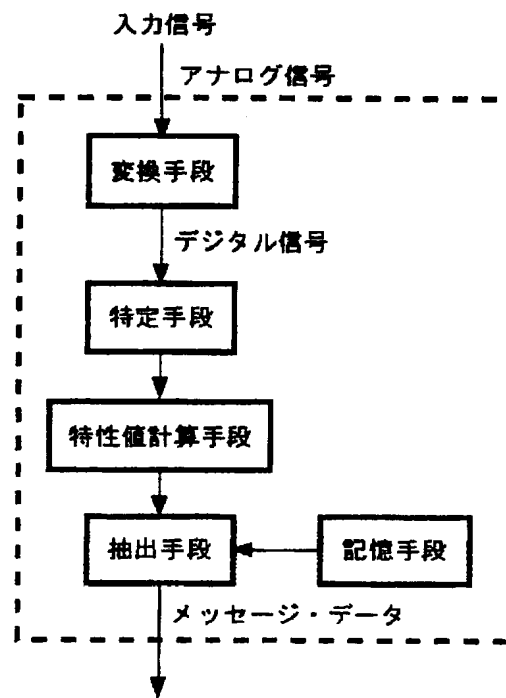


FIG. 22

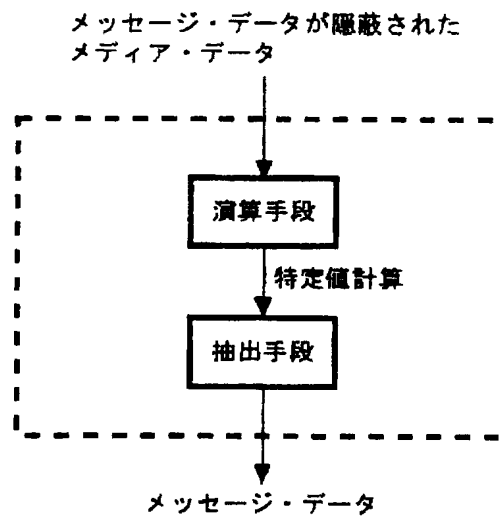


FIG. 23

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP97/00395

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl⁶ H04N1/387

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl⁶ H04N1/00-1/64, G06T1/00-17/50, G09C5/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1926 - 1997

Kokai Jitsuyo Shinan Koho 1971 - 1997

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 6-22119, A (Minolta Camera Co., Ltd.), January 28, 1994 (28. 01. 94) (Family: none)	1 - 66
A	JP, 7-123244, A (Toshiba Corp.), May 12, 1995 (12. 05. 95) & EP, 642060, A	1 - 66
A	JP, 63-214067, A (Toyo Communication Equipment Co., Ltd.), September 6, 1988 (06. 09. 88) (Family: none)	1 - 66

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
April 28, 1997 (28. 04. 97)Date of mailing of the international search report
May 13, 1997 (13. 05. 97)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.⁶ H04N1/387

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.⁶ H04N1/00-1/64, G06T1/00-17/50, G09C5/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1997年
 日本国公開実用新案公報 1971-1997年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP, 6-22119, A (ミノルタカメラ株式会社), 28. 1月. 1994 (28. 01. 94) (ファミリーなし)	1-66
A	JP, 7-123244, A (株式会社東芝), 12. 5月. 1995 (12. 05. 95) & EP, 642060, A	1-66
A	JP, 63-214067, A (東洋通信機株式会社), 6. 9月. 1988 (06. 09. 88) (ファミリーなし)	1-66

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 先行文献ではあるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

28. 04. 97

国際調査報告の発送日

13.05.97

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
 郵便番号100

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

乾 雅浩

5C

9562

電話番号 03-3581-1101 内線 3543